# PATENT ABSTRACTS OF JAPAN

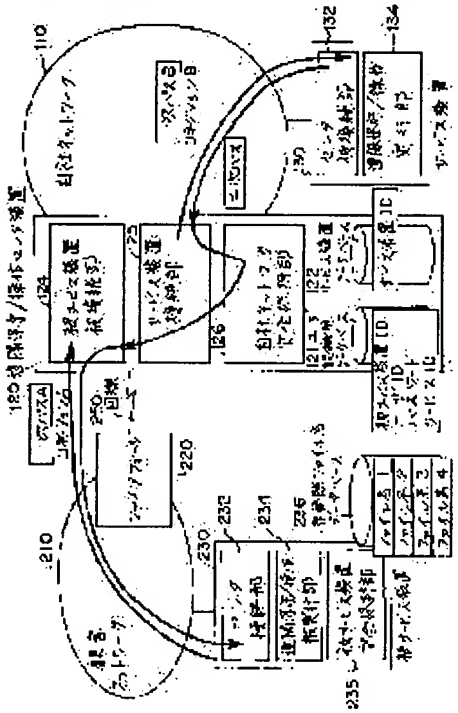
(11)Publication number : **08-314835**
(43)Date of publication of application : **29.11.1996**

(51)Int.Cl. G06F 13/00
G06F 11/30
H04Q 9/00
H04Q 9/00

(21)Application number : **07-121975**
(22)Date of filing : **19.05.1995**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **TANNO IPPEI**

## (54) DEVICE TO RECEIVE SERVICE, CENTER DEVICE, SERVICE DEVICE AND REMOTE CONTROL SYSTEM



(57)Abstract:
PURPOSE: To execute remote control between a service device and a device to receive service connected to an internal network where fire walls are mutually installed.
CONSTITUTION: The device 230 to receive service establishes connection A with a remote maintenance/control center device 120 through a customer network 210 and a fire wall 220. Next, the device 230 to receive service transmits security check information through the connection A to the remote maintenance/ control center device 120. The remote maintenance/control center device 120 checks this security check information by retrieving a data base 121 for user certification and when it is confirmed that the contracted user owns the device 230 to receive service, connection B with the service device 130 is established through its own company network 110. Thus, the service device 130 can remotely maintain/control the device 230 to receive service through a logical path composed of the connection A and the connection B.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

**特開平8－314835**

(43)公開日　平成８年(1996)11月29日

| (51)Int.Cl.[6] | 識別記号 | 庁内整理番号 | ＦＩ | | 技術表示箇所 |
|---|---|---|---|---|---|
| Ｇ０６Ｆ　13/00 | ３５１ | 7368－5E | Ｇ０６Ｆ　13/00 | ３５１Ｚ | |
| 11/30 | | 7313－5B | 11/30 | Ｄ | |
| Ｈ０４Ｑ　9/00 | ３０１ | | Ｈ０４Ｑ　9/00 | ３０１Ｚ | |
| | ３２１ | | | ３２１Ｚ | |

審査請求　未請求　請求項の数20　ＯＬ　（全 31 頁）

(21)出願番号　特願平7－121975

(22)出願日　平成７年(1995)５月19日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(72)発明者　丹野　一平
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

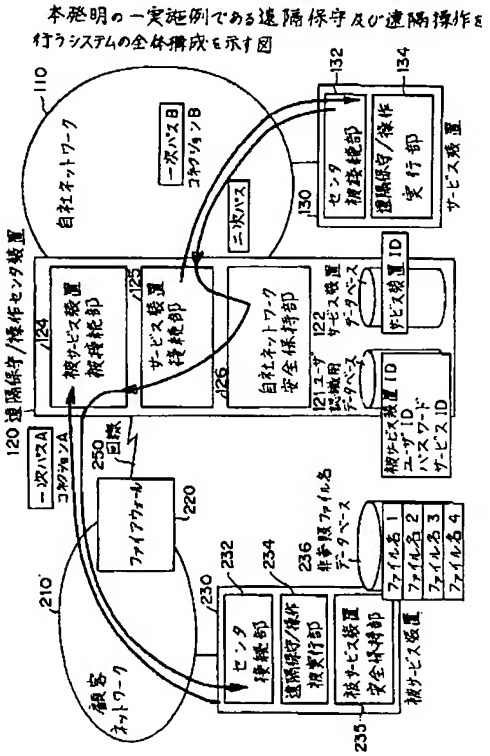
(74)代理人　弁理士　大菅　義之　（外１名）

(54)【発明の名称】　被サービス装置、センタ装置、サービス装置、及び遠隔操作システム

(57)【要約】

【目的】　本発明は、互いにファイアウォールが設置されている内部ネットワークに接続されたサービス装置と被サービス装置との間で、遠隔操作を実施できるようにすることを目的とする。

【構成】　被サービス装置２３０は、顧客ネットワーク２１０及びファイアウォール２２０を介して遠隔保守／操作センタ装置１２０とコネクションＡを確立する。次に、被サービス装置２３０は、該コネクションＡを介して遠隔保守／操作センタ装置１２０にセキュリティ・チェック情報を送信する。遠隔保守／操作センタ装置１２０は、このセキュリティ・チェック情報をユーザ認証用データベース１２１を検索してチェックし、上記被サービス装置２３０が契約先のユーザのものであると確認した場合には、自社ネットワーク１１０を介してサービス装置１３０とコネクションＢを確立する。これにより、サービス装置１３０は、上記コネクションＡとコネクションＢによって構成される論理的なパスを介して、被サービス装置２３０を遠隔保守／操作することができるようになる。



1

【特許請求の範囲】

【請求項1】　外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するパケット通信手段と、

該パケット通信手段が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

を備えたことを特徴とする被サービス装置。

【請求項2】　外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第二のファイアウォールを介して前記第一のファイアウォールとの間にコネクションを確立し、該コネクションを介して該第一のファイアウォールとの間でパケットを送受信するパケット通信手段と、

該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

該遠隔操作実行手段によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段と、

を備えたことを特徴とする被サービス装置。

【請求項3】　インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、該インターネットを介して遠隔操作サービスを実施される、該インターネットに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するパケット通信手段と、

該パケット通信手段が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

を備えたことを特徴とする被サービス装置。

2

【請求項4】　インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、該インターネットを介して遠隔操作サービスを実施される、該インターネットに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置において、

前記第二のファイアウォールを介して前記第一のファイアウォールとの間にコネクションを確立し、該コネクションを介して該第一のファイアウォールとの間でパケットを送受信するパケット通信手段と、

該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する遠隔操作実行手段と、

該遠隔操作実行手段によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段と、

を備えたことを特徴とする被サービス装置。

【請求項5】　外部ネットワークに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該外部ネットワークに対する第二のファイアウォールとして機能するセンタ装置において、

前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する第一のパケット通信手段と、

前記第一のコネクションが確立された後に、該第一のパケット通信手段によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックするセキュリティ・チェック手段と、

該セキュリティ・チェック手段によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記

3

自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する第二のパケット通信手段と、
を備えたことを特徴とするセンタ装置。

【請求項6】　契約先のユーザの認証情報が登録されたデータベースをさらに備え、
前記セキュリティ・チェック手段は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否をかをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断すること、
を特徴とする請求項5記載のセンタ装置。

【請求項7】　前記第二のコネクションを確立するために使用するサービス装置の識別情報が登録されたデータベースをさらに備え、
前記第二のパケット通信手段は、前記第一のパケット通信手段によって受信されたパケットに格納されているサービス識別情報に対応するサービス装置識別情報を前記第二のデータベースから取り出し、このサービス装置識別情報を用いて前記第二のコネクションを確立すること、
を特徴とする請求項5記載のセンタ装置。

【請求項8】　インターネットに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該インターネットに対する第二のファイアウォールとして機能するセンタ装置において、
インターネットに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置に対して、該インターネットを介して遠隔操作サービスを実施する業者の内部ネットワークの該インターネットに対する第二のファイアウォールとして機能するセンタ装置において、
前記第一のファイアウォールと前記インターネットを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する第一のパケット通信手段と、
前記第一のコネクションが確立された後に、該第一のパケット通信手段によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックするセキュリティ・チェック手段と、
該セキュリティ・チェック手段によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する第二のパケット通信手段と、

4

を備えたことを特徴とするセンタ装置。

【請求項9】　契約先のユーザの認証情報が登録されたデータベースをさらに備え、
前記セキュリティ・チェック手段は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否をかをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断すること、
を特徴とする請求項8記載のセンタ装置。

【請求項10】　前記第二のコネクションを確立するために使用するサービス装置のＩＰアドレスが登録されたデータベースをさらに備え、
前記第二のパケット通信手段は、前記第一のパケット通信手段によって受信されたパケットに格納されているサービス識別情報に対応するＩＰアドレスを前記第二のデータベースから取り出し、このＩＰアドレスを用いて前記第二のコネクションを確立すること、
を特徴とする請求項8記載のセンタ装置。

【請求項11】　外部ネットワークに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記外部ネットワークに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置において、
前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信するパケット通信手段と、
該パケット通信手段によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドが設定されたパケットを生成し、このパケットを、前記パケット通信手段を介して、前記第二のファイアウォールに送信する遠隔操作実行手段と、
を備えることを特徴とするサービス装置。

【請求項12】　前記遠隔操作実行手段は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力すること、を特徴とする請求項11記載のサービス装置。

【請求項13】　インターネットに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記インターネットに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置において、
前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信するパケット通信手段と、

5

該パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の指示情報を取り出し、該指示情報によって指示される遠隔操作を実施するためのコマンドが設定されたパケットを生成し、このパケットを前記第二のファイアウォールに送信する遠隔操作実行手段と、

を備えることを特徴とするサービス装置。

【請求項１４】　前記遠隔操作実行手段は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力すること、を特徴とする請求項１３記載のサービス装置。

【請求項１５】　顧客の内部ネットワークと遠隔操作を提供する業者の内部ネットワークが外部ネットワークを介して接続されており、かつ、上記二つの内部ネットワークに対して前記外部ネットワークに対するファイアウォールが設置されているシステムを利用して、上記顧客の内部ネットワークに接続された被サービス装置を、上記遠隔操作を提供する業者の内部ネットワークに接続されたサービス装置によって遠隔操作するサービスを実施する遠隔操作サービスシステムにおいて、

前記被サービス装置は、

前記顧客ネットワーク及び該顧客ネットワークに対する第一のファイアウォールを介して、前記遠隔操作サービス提供業者の内部ネットワークに対して設置された第二のファイアウォールに第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置と遠隔操作を実施するためのデータが格納されているパケットを送受信し、

前記第二のファイアウォールは、

前記被サービス装置と前記第一のコネクションを確立した後に、自社の内部ネットワークを介して前記サービス装置と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置と前記サービス装置との間で授受されるパケットを中継し、

前記サービス装置は、

前記被サービス装置との間で授受するパケットを、前記第二のファイアウォールと前記第二のコネクションを介して送受信することにより、前記被サービス装置に対して遠隔操作のサービスを実施すること、

を特徴とする遠隔操作サービスシステム。

【請求項１６】　前記第二のファイアウォールは、

前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置が契約先のユーザのものであるか否かを認証する認証手段を、

を備えることを特徴とする請求項１５記載の遠隔操作サービスシステム。

6

【請求項１７】　前記被サービス装置は、

前記第二のファイアウォールから、前記第一のコネクションを介して前記サービス装置から送信されてきたパケットを受信した際に、そのパケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、

備えることを特徴とする請求項１５記載の遠隔操作実行システム。を備えることを特徴とするサービス装置。

【請求項１８】　顧客の内部ネットワークと遠隔操作を提供する業者の内部ネットワークがインターネットを介して接続されており、かつ、上記二つの内部ネットワークに対して前記インターネットに対するファイアウォールが設置されているシステムを利用して、上記顧客の内部ネットワークに接続された被サービス装置を、上記遠隔操作を提供する業者の内部ネットワークに接続されたサービス装置によって遠隔操作するサービスを実施する遠隔操作サービスシステムにおいて、

前記被サービス装置は、

前記顧客ネットワーク及び該顧客ネットワークに対する第一のファイアウォールを介して、前記遠隔操作サービス提供業者の内部ネットワークに対して設置された第二のファイアウォールに第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置と遠隔操作を実施するためのデータが格納されているパケットを送受信し、

前記第二のファイアウォールは、

前記被サービス装置と前記第一のコネクションを確立した後に、自社の内部ネットワークを介して前記サービス装置と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置と前記サービス装置との間で授受されるパケットを中継し、

前記サービス装置は、

前記被サービス装置との間で授受するパケットを、前記第二のファイアウォールと前記第二のコネクションを介して送受信することにより、前記被サービス装置に対して遠隔操作のサービスを実施すること、

を特徴とする遠隔操作サービスシステム。

【請求項１９】　前記第二のファイアウォールは、

前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置が契約先のユーザのものであるか否かを認証する認証手段を、

を備えることを特徴とする請求項１８記載の遠隔操作サービスシステム。

【請求項２０】　前記被サービス装置は、

前記第二のファイアウォールから、前記第一のコネクションを介して前記サービス装置から送信されてきたパケットを受信した際に、そのパケットに格納されている遠

隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、
備えることを特徴とする請求項１８記載の遠隔操作実行システム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、インターネットなどのオープンな外部ネットワークを介して、ユーザ側のネットワークに接続された装置を、自社内のネットワークに接続されたサービス装置によって遠隔操作しながら保守・管理等を行う遠隔操作方式に係わり、特に、互いのネットワークに対してファイアウォールが設けられている場合における遠隔操作方式に関する。

【０００２】

【従来の技術】最近では、出張経費及びそれに伴う時間の節約などのために、ユーザの装置の保守や管理作業を、ネットワークを介して、遠隔操作により行う方式が盛んになりつつある。

【０００３】また、この遠隔操作のためのネットワークとしてインターネットを利用する方式の採用も試みられるようになっている。インターネットは、世界的なネットワークであり、世界中の不特定の相手と自由に通信することが可能である。したがって、インターネットを利用することにより、グローバルな遠隔保守作業が可能となる。

【０００４】ところで、インターネットは、オープンなネットワークであるがために、セキュリティの点で問題がある。特に、企業が社内ネットワークをインターネットに接続する場合、該社内ネットワークに接続された全てのホストがインターネットを介して部外者からアクセス可能となるので、極秘すべき重要な内部情報が盗まれたり、システムがクラッシュさせられたり、さらにはデータが変更させられるなどの危険にさらされることになる。

【０００５】このため、最近では、インターネットと社内ネットワークとの間に”ファイアウォール”を設けるようになってきている。ファイアウォールは、不法な侵入者から社内ネットワークを保護するための機構であり、一般に、パケットフィルタリングゲートウェイ、サーキットゲートウェイ、及びアプリケーションゲートウェイに大別される。

【０００６】図ｊ１は、外部ネットワーク（インターネット）１と内部ネットワーク２（社内ネットワーク）との間に設置された上記パケットフィルタリングゲートウェイ機能を備えたファイアウォール３の概略構成を示す図である。同図には、ＩＰアドレス・フィルタリングとＴＣＰポート・フィルタリングの例が示されている。

【０００７】インターネット上の通信は、ＴＣＰ／ＩＰプロトコルをベースにして行われており、ＩＰデータグラム（ＩＰパケット）がインターネット内をパケツリレーの形でルーティング制御される。該ＩＰデータグラムは、そのヘッダ部分にＩＰヘッダとＴＣＰヘッダを含んでいる。

【０００８】ＩＰヘッダは、ＩＰ宛先アドレス（図中の受信ＩＰアドレス）とＩＰ送信元アドレス（図中の発進ＩＰアドレス）を含んでいる。このＩＰアドレスは、ネットワーク・アドレスとホスト・アドレスから構成されている。

【０００９】また、ＴＣＰヘッダは、受信ポート番号と発信ポート番号を含んでいる。このポート番号はプロセスに１対１に対応するもので、インターネットを介したプロセス間通信に利用される。

【００１０】ファイアウォール３は、その内部にＩＰアドレス登録テーブル３２とポート番号登録テーブル３４を備えている。ＩＰアドレス登録テーブル３２には、内部ネットワーク２に通過させてもよいＩＰアドレスの組が登録されている。また、ポート番号登録テーブル３４には、内部ネットワーク２に通過させてもよいポート番号の組が登録されている。

【００１１】上記ＩＰアドレス・フィルタリングでは、パケットを受信すると、上記ＩＰアドレス登録テーブル３２を参照して、そのパケットのＩＰデータグラムに、テーブル３２に登録されていない発信ＩＰアドレスがＩＰヘッダに設定されているＩＰデータグラムを棄却する。また、ＴＣＰポート・フィルタリングでは、ＩＰデータグラム（パケット）を受信すると、上記ポート番号登録テーブル３４を参照して、そのテーブル３４に登録されていないポート番号の組がＴＣＰヘッダに設定されているＩＰデータグラムを棄却する。これにより、Ｔｅｌｎｅｔ，ＦＴＰなどの特定のアプリケーションをフィルタリングできる。

【００１２】また、図ｊ２は、ファイアウォール３の第２の機能を説明する図である。ファイアウォール３は、外部ネットワーク１（インターネットなど）上のホストが、内部ネットワーク２内のホスト（内部ホスト）を直接アクセスできないようにするために、内部ネットワーク２内のホストのアクセスを代行する機能を備えている。すなわち、内部ネットワーク２内のホストが外部ネットワーク１にアクセスする際には、常に、ファイアウォール３を介して行うようにする。

【００１３】同図の例では、ファイアウォール３に対して、”Ｅ”のＩＰアドレスが設定されている。また、内部ネットワーク２内の各ホストＡ，Ｂ，Ｃ，及びＤに対して、それぞれ、”Ａ”、”Ｂ”，”Ｃ”，及び”Ｄ”のＩＰアドレスが設定されている。このようなシステムにおいて、ホストＢが外部ネットワーク１上のあるホスト（外部ホスト）に対してＩＰデータグラム１２を送信する場合、このＩＰデータグラム１２をファイアウォール３に送信する。したがって、このＩＰデータグラム１２の発信ＩＰアドレスは”Ｂ”に設定される。ファイア

ウォール３は、このＩＰデータグラム１２を受信すると、その発信ＩＰアドレスを，自己のＩＰアドレスである”Ｅ”に変換して、外部ネットワーク１に送出する。

【００１４】このように、外部ネットワーク１に対してはファイアウォール３のみを公開するようにして、内部ネットワーク２の存在を外部ネットワーク１に知らせないようにする。尚、この機能はＩＰ中継機能とも呼ばれる。

【００１５】以上述べたようなパケットフィルタリングゲートウェイ機能を備えたファイアウォール３を内部ネットワーク２と外部ネットワーク１との間に設置することにより、外部ネットワーク１を介して、直接、内部ネットワーク２内に侵入しようとする不法なＩＰデータグラムを、ほぼ完全にブロックすることが可能になる。

【００１６】図ｊ３は、Ａ社、Ｂ社、Ｃ社、及びＤ社のネットワーク２Ａ，２Ｂ，２Ｃ，および２Ｄが商用インターネット５に接続されたシステムを示す図である。このシステムにおいて、Ａ社、Ｂ社、Ｃ社、及びＤ社は、それぞれの内部ネットワーク２Ａ，２Ｂ，２Ｃ，および２Ｄを、商用インターネット５を介する外部からの不法アクセスから守るために、該商用インターネット５と自社の内部ネットワーク２Ａ，２Ｂ，２Ｃ，および２Ｄとの間にファイアウォール３Ａ，３Ｂ，３Ｃ，及び３Ｄを設置している。

【００１７】

【発明が解決しようとする課題】次に、上記図ｊ３に示すようなシステムにおいて発生する問題点を、図ｊ４を参照しながら説明する。

【００１８】図ｊ４において、Ａ社が顧客が運営するネットワーク内の装置やソフトウェアなどに対する保守や作業代行などのサービスを実施する会社であり、該顧客先がＤ社であったとする。この場合、Ａ社が自社ネットワークに接続されたサービス装置６を用いて、Ｄ社のネットワーク２Ｄに接続された被サービス装置７の保守や作業代行を、商用インターネット５を介する遠隔操作により実施したいと考えたとする。

【００１９】この場合、Ａ社のサービス装置６が商用インターネット５を介して、Ｄ社の被サービス装置７に該遠隔操作用のパケットを送信しても、例えばＡ社のファイアウォール３ＡのＩＰアドレスが，Ｄ社のファイアウォール３ＤのＩＰアドレス登録テーブル３２に登録されていない場合には、上記サービス装置６がＤ社のファイアウォール３Ｄに送信したパケットは、ファイアウォール３Ｄによって棄却されてしまい、Ｄ社の内部ネットワーク２Ｄに入り込むことができない。このため、Ａ社ではＤ社の被サービス装置７に対して保守や作業代行等のサービスを実施することができない。

【００２０】また、Ｄ社のファイアウォール３ＤのＩＰアドレス登録テーブル３２に、Ａ社のファイアウォール３ＡのＩＰアドレスを登録すれば、Ａ社のサービス装置６がＤ社の被サービス装置７を遠隔操作して、その装置７の保守や作業を実行できるようになるが、これは、セキュリティの点で問題がある。すなわち、この場合、Ａ社のサービス装置６以外のホストを操作することにより、Ｄ社の内部ネットワーク２Ｄのシステムを破壊したり、重要な情報を盗まれる可能性がある。何故ならば、Ｄ社のファイアウォール３Ｄは、商用インターネット５を介して受信するＡ社のファイアウォール３Ａから送られてくるパケットを、Ａ社のいずれのホストが発信したパケットであるか特定できないからである。

【００２１】このため、従来は、図ｊ５に模式的に示すように、公衆回線８または専用線により、Ａ社のサービス装置６と顧客であるＤ社の被サービス装置７を、直接二点間接続して、被サービス装置７の保守や作業代行を実施していた。しかしながら、このような方式を用いると、Ａ社及びＤ社が共に、該直接二点間接続するための専用の通信装置９Ａ，９Ｄなどの装備やサービス授受専用の環境を用意する必要があり、両社が二重投資をせねばならずコストの増大をもたらし、好ましくない。また、さらに、サービス実施時には、社内のネットワークのセキュリティを保持するために、サービス装置６と被サービス装置７とも、それぞれの社内ネットワーク２Ａ，２Ｄから切り離し、サービスが終了した時点で、再び、それらの装置６、７をそれぞれの社内ネットワーク２Ａ，２Ｄに接続するという煩雑な作業が必要となる。

【００２２】本発明は、互いにファイアウォールを設置している遠隔操作により保守や管理サービスを実施する会社と該サービスを受ける会社の双方が、自社のネットワークのセキュリティを保持しつつ、安価な設備投資で、遠隔保守や遠隔操作を実施できるシステムを実現することを目的とする。

【００２３】

【課題を解決するための手段】図１は本発明の原理を説明する図（その１）である。図１に示す発明（第一の発明）は、外部ネットワークに対する第一のファイアウォールが設置された遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置によって、該外部ネットワークを介して遠隔操作サービスを実施される、該外部ネットワークに対する第二のファイアウォールが設置された自社の内部ネットワークに接続された被サービス装置を前提とする。

【００２４】パケット通信手段５１は、前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信するまた、第二の発明は、上記パケット通信手段５１と遠隔操作実行手段５２に加え、さらに、遠隔操作実行手段５２によって実行された遠隔操作の実

行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する実行結果返信手段５３と、該パケット通信手段５１によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックするセキュリティ・チェック手段５４を備える。この場合、遠隔操作実行手段５２は、セキュリティ・チェック手段５４によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する。

【００２５】前記第一及び第二の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図２は、本発明の原理を説明する図（その２）である。

【００２６】この図２に示す第三の発明は、外部ネットワークに対する第一のファイアウォールが設置された契約先のユーザの内部ネットワークに接続された被サービス装置に対して、該外部ネットワークを介して遠隔操作サービスを実施する業者の内部ネットワークの該外部ネットワークに対する第二のファイアウォールとして機能するセンタ装置を前提とする。

【００２７】第一のパケット通信手段６１は、前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する。

【００２８】セキュリティ・チェック手段６２は、前記第一のコネクションが確立された後に、第一のパケット通信手段６１によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックする。

【００２９】第二のパケット通信手段６３は、セキュリティ・チェック手段６２によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する。

【００３０】また、上記第三の発明において、契約先のユーザの認証情報が登録されたデータベースをさらに備え、前記セキュリティ・チェック手段６２は、前記受信パケットに該データベースに登録されている認証情報が格納されているか否をかをチェックすることにより、前記受信パケットが契約先のユーザからのものであるか否かを判断するような構成にしてもよい。

【００３１】また、上記第三の発明において、前記第二のコネクションを確立するために使用するサービス装置の識別情報が登録されたデータベースをさらに備え、前記第二のパケット通信手段６３は、前記第一のパケット通信手段６１によって受信されたパケットに格納されているサービス識別情報に対応するサービス装置識別情報を前記第二のデータベースから取り出し、このサービス装置識別情報を用いて前記第二のコネクションを確立するような構成にしてもよい。

【００３２】また、前記第三の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図３は、本発明の原理を説明する図（その３）である。

【００３３】この図３に示す第四の発明は、外部ネットワークに対して第一のファイアウォールが設置された顧客の内部ネットワークに接続された被サービス装置に対して遠隔操作サービスを実施する、上記外部ネットワークに対して第二のファイアウォールが設置された自社の内部ネットワークに接続されたサービス装置を前提とする。

【００３４】パケット通信手段７１は、前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信する。

【００３５】遠隔操作実行手段７１は、該パケット通信手段７１によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドが設定されたパケットを生成し、このパケットを、前記パケット通信手段を介して、前記第二のファイアウォールに送信する。

【００３６】上記第四の発明において、例えば、前記遠隔操作実行手段７２は、前記パケット通信手段によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力する。

【００３７】前記第四の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。図４は、本発明の原理を説明する図（その４）である。

【００３８】この図５に示す第五の発明は、顧客の内部ネットワーク８２と遠隔操作を提供する業者の内部ネットワーク８６が外部ネットワーク８４を介して接続されており、かつ、上記二つの内部ネットワーク８２、８６に対して前記外部ネットワーク８４に対するファイアウォール８３、８５が設置されているシステムを利用して、上記顧客の内部ネットワーク８２に接続された被サービス装置８１を、上記遠隔操作を提供する業者の内部ネットワーク８６に接続されたサービス装置８７によって遠隔操作するサービスを実施する遠隔操作サービスシステムを前提とする。

【００３９】そして、前記被サービス装置８１は、前記顧客ネットワーク８２及び該顧客ネットワーク８２に対する第一のファイアウォール８３を介して、前記遠隔操作サービス提供業者の内部ネットワーク８６に対して設置された第二のファイアウォール８５に第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワーク８６に接続さ

れたサービス装置８７と遠隔操作を実施するためのデータが格納されているパケットを送受信し、前記第二のファイアウォール８５は、前記被サービス装置８１と前記第一のコネクションを確立した後に、自社の内部ネットワーク８６を介して前記サービス装置８７と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置８１と前記サービス装置８７との間で授受されるパケットを中継し、前記サービス装置８７は、前記被サービス装置８１との間で授受するパケットを、前記第二のファイアウォール８５と前記第二のコネクションを介して送受信することにより、前記被サービス装置８１に対して遠隔操作のサービスを実施することを特徴とする。

【００４０】上記第五の発明において、前記第二のファイアウォール８５は、例えば、前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置８１が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置８１が契約先のユーザのものであるか否かを認証する認証手段を、を備えるような構成にしてもよい。

【００４１】また、上記第五の発明において、前記被サービス装置８１は、前記第二のファイアウォール８５から、前記第一のコネクションを介して前記サービス装置８７から送信されてきたパケットを受信した際に、そのパケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する認証手段を、備えるような構成にしてもよい。

【００４２】前記第五の発明において、前記外部ネットワークは、例えば、インターネットであってもよい。

【００４３】

【作用】第一の発明では、パケット通信手段５１が、前記第一のファイアウォールが内部ネットワークに接続されたサービス装置のアドレスを特定するための識別子を送信し、前記第二のファイアウォール及び第一のファイアウォールを介して、前記サービス装置との間にコネクションを確立し、該コネクションを介して該サービス装置との間でパケットを送受信する。そして、遠隔操作実行手段５２は、パケット通信手段５１が受信したパケットから遠隔操作の指示情報を取り出し、該指示情報の指示に従って自装置の遠隔操作を実行する。

【００４４】したがって、遠隔操作サービス提供業者の内部ネットワークと顧客ネットワークが、互いに外部ネットワークに対してファイアウォールを設置していている内部ネットワークに接続された被サービス装置は、遠隔操作サービス提供業者の内部ネットワーク内部に自己が生成したパケットを送信できると共に、遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置からパケットを受信できる。

【００４５】また、第二の発明では、セキュリティ・チェック手段５４が、該パケット通信手段５１によって受信されたパケットに格納されている遠隔操作の指示情報の安全性をチェックする。そして、遠隔操作実行手段５２は、セキュリティ・チェック手段５４によって安全性が確認された遠隔操作の指示情報の指示に従って自装置の遠隔操作を実行する。そして、実行結果返信手段５３が、遠隔操作実行手段５２によって実行された遠隔操作の実行結果を、前記パケット通信手段を介して前記第一のファイアウォールに送信する。

【００４６】したがって、被サービス装置は、その安全性を保持しながら、遠隔操作のサービスを受けることができると。また、サービス装置は、第一のファイアウォールを介して、被サービス装置において実施された遠隔操作の実行結果を得ることができる。

【００４７】また、第三の発明では、第一のパケット通信手段６１が、前記第一のファイアウォールと前記外部ネットワークを介して前記被サービス装置との間に第一のコネクションを確立し、該第一のコネクションを介して前記被サービス装置との間でパケットを送受信する。そして、セキュリティ・チェック手段６２は、前記第一のコネクションが確立された後に、第一のパケット通信手段６１によって受信されたパケットが契約先のユーザの被サービス装置から送信されてきたパケットであるか否かをチェックする。続いて、第二のパケット通信手段６３は、セキュリティ・チェック手段６２によって前記パケットが契約先のユーザの被サービス装置から送信されてきたパケットであることが確認された場合に、自社の内部ネットワークを介して前記サービス装置との間に第二のコネクションを確立し、該第二のコネクションを介して前記自社の内部ネットワークに接続されたサービス装置との間でパケットを送受信する。

【００４８】したがって、第一のファイアウォールが設置されている顧客の内部ネットワークに接続された被サービス装置との間でパケットの送受信をすることができる。また、受信するパケットのセキュリティ・チェックを行い、不当なパケットを棄却することができる。そして、自社の内部ネットワークに接続されたサービス装置に正規の契約先のユーザの被サービス装置から送信されてきたパケットのみを送信することができる。また、上記サービス装置から上記顧客の被サービス装置に送られるパケットを、該被サービス装置に送信することができる。

【００４９】また、第四の発明では、パケット通信手段７１が、前記第二のファイアウォールとコネクションを確立し、該コネクションを介して前記被サービス装置との間で授受するデータが格納されているパケットを送受信する。そして、遠隔操作実行手段７２は、該パケット通信手段７１によって受信されたパケットに格納されている遠隔操作の指示情報によって指示される遠隔操作を、被サービス装置に対して実施するためのコマンドが設定されたパケットを生成し、このパケットを、前記パ

ケット通信手段７１を介して、前記第二のファイアウォールに送信する。また、さらに、例えば、前記遠隔操作実行手段７２は、前記パケット通信手段７１によって受信されたパケットから前記被サービス装置が設定した遠隔操作の実行結果を取り出し、これを外部出力する。

【００５０】したがって、遠隔操作サービス提供業者の内部ネットワークに接続されたサービス装置は、外部ネットワークに対して設置された第二のファイアウォールとパケットを送受信することができる。このため、第二のファイアウォールが顧客の内部ネットワークに接続された被サービス装置との間にコネクションを確立することにより、上記サービス装置は、被サービス装置と遠隔操作のサービスを実施するためにパケットを送受信することができる。

【００５１】また、第五の発明では、被サービス装置８１が、前記顧客ネットワーク８２及び該顧客ネットワーク８２に対する第一のファイアウォール８３を介して、前記遠隔操作サービス提供業者の内部ネットワーク８６に対して設置された第二のファイアウォール８５に第一のコネクションを確立し、該第一のコネクションを介して前記遠隔操作サービス提供業者の内部ネットワーク８６に接続されたサービス装置８７と遠隔操作を実施するためのデータが格納されているパケットを送受信する。

【００５２】また、第二のファイアウォール８５は、前記被サービス装置８１と前記第一のコネクションを確立した後に、自社の内部ネットワーク８６を介して前記サービス装置８７と第二のコネクションを確立し、これら第一及び第二のコネクションを利用して、前記被サービス装置８１と前記サービス装置８７との間で授受されるパケットを中継する。

【００５３】さらに、サービス装置８７は、　前記被サービス装置８１との間で授受するパケットを、前記第二のファイアウォール８５と前記第二のコネクションを介して送受信することにより、前記被サービス装置８１に対して遠隔操作のサービスを実施する。

【００５４】この場合、例えば、前記第二のファイアウォール８５は、内部の認証手段により、前記第一のコネクションが確立された後に、該第一のコネクションを介して前記被サービス装置８１が送信してくるパケットに設定されているデータの内容を基に、前記被サービス装置８１が契約先のユーザのものであるか否かを認証する。

【００５５】また、例えば、前記被サービス装置８１は、内部の認証手段により、前記第二のファイアウォール８５から、前記第一のコネクションを介して前記サービス装置８７から送信されてきたパケットを受信した際に、そのパケットに格納されている遠隔操作実行用のコマンドが正当なコマンドであるか否かを認証する。

【００５６】したがって、顧客の内部ネットワーク８２と遠隔操作サービス提供業者の内部ネットワーク８６が、それぞれが接続されている外部ネットワーク８４に対して互いに第一のファイアウォール８３、第二のファイアウォール８５を設置しているシステムにおいて、顧客及び遠隔操作サービス提供業者がそれぞれの内部ネットワークのセキュリティの安全性を保持したままで、サービス装置８７が顧客の被サービス装置８１に対して、遠隔操作のサービスを実施することができる。

【００５７】

【実施例】以下、図面を参照しながら、本発明の実施例を説明する。図５は、本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図である。

【００５８】同図において、自社ネットワーク１１０は、上記遠隔保守及び遠隔操作のサービスを実施する業者であるＡ社の社内ネットワークであり、顧客ネットワーク２１０は該サービスを受けるユーザであるＤ社の社内ネットワークである。

【００５９】Ａ社の自社ネットワーク１１０とＤ社の顧客ネットワーク２１０は、公衆回線または商用インターネットなどの回線２５０によって互いに接続されている。但し、Ａ社の自社ネットワーク１１０と回線２５０との間にはファイアウォールとして機能する遠隔保守／操作センタ装置１２０が設置され、また、顧客ネットワーク２１０と回線２５０との間にはファイアウォール２２０が設置されている。

【００６０】自社ネットワーク１１０には、遠隔保守及び遠隔操作のサービスを実行するサービス装置１３０が接続されている。また、顧客ネットワーク２１０には、該サービス装置１３０によって上記遠隔保守及び遠隔操作のサービスを受ける被サービス装置２３０が接続されている。

【００６１】遠隔保守／操作センタ装置１２０は、自社ネットワーク１１０のサービス装置１３０に対して顧客ネットワーク２１０に接続された被サービス装置２３０にパケット（ＩＰデータグラム）の中継処理を提供する。また、自社ネットワーク１１０のセキュリティを保持するためにユーザ認証機能を備えている。このユーザ認証機能は、ユーザ認証用データベース１２１を備えることによって実現されている。

【００６２】ユーザ認証用データベース１２１は、被サービス装置ＩＤ，ユーザＩＤ，パスワード、及びサービスＩＤの４種類の情報を、サービスを提供する各被サービス装置２３０毎に、個別に、記憶している。

【００６３】また、遠隔保守／操作センタ装置１２０は、サービス装置データベース１２２も備えている。このサービス装置データベース１２２は、上記ユーザ認証用データベース１２１に登録されているサービスＩＤを有するサービス装置１３０のＩＰアドレスを記憶している。

【００６４】また、さらに、遠隔保守／操作センタ装置

１２０は、被サービス装置被接続部１２４、サービス装置接続部１２５、及び自社ネットワーク安全保持部１２６を備えている。

【００６５】被サービス装置被接続部１２４は、顧客ネットワーク２１０に接続されている被サービス装置２３０との間でファイアウォール２２０を介して、ＴＣＰプロコトルにより論理的なパスであるコネクション（コネクションＡ）を確立する。尚、この場合、該コネクションＡの確立要求は、顧客ネットワーク２１０に接続された被サービス装置２３０側からなされる。被サービス装置被接続部１２４は、このコネクションＡによって設定されたパスＡを利用することにより、サービス装置１３０から送出される被サービス装置２３０宛のパケットをファイアウォール２２０を通過させ、顧客ネットワーク２１０を介して被サービス装置２３０に届けさせる。

【００６６】サービス装置接続部１２５は、該被サービス装置被接続部１２４からの依頼を受けて、遠隔保守／操作センタ装置１２０とサービス装置１３０との間に、自社ネットワーク安全保持部１２６を介してＴＣＰプロコトルにより論理的なパスであるコネクション（コネクションＢ）を確立させる。但し、このコネクションＢの確立要求は、上記コネクションＡが確立された後に、被サービス装置２３０が上記パスＡにより送ってくるパケットのデータ部に含まれるサービスＩＤ，ユーザＩＤ，被サービス装置ＩＤ，及びパスワードによって、被サービス装置２３０が正しい契約ユーザの装置であると認識された後に、なされる。

【００６７】自社ネットワーク安全保持部１２６は、該サービス装置接続部１２４からの依頼を受けて、上述した被サービス装置２３０が契約ユーザであるかのの認証処理を、前記ユーザ認証用データベース１２１を参照することにより実行する。そして、その認証結果を被サービス装置被接続部１２４に返す。

【００６８】サービス装置１３０は、センタ被接続部１３２と遠隔保守／操作実行部１３４を備えている。センタ被接続部１３２は、自社ネットワーク１１０を介して遠隔保守／操作センタ装置１２０内のサービス装置接続部１２５との間で前記コネクションＢを確立する。そして、該コネクションＢによって設定されたパスＢを介して、該サービス装置接続部１２５から被サービス装置２３０が送信してきた遠隔保守／操作要求のパケットを受け取る。そして、この要求を遠隔保守／操作実行部１３４に伝える。また、該遠隔保守／操作実行部１３４から依頼される遠隔保守／操作実行用のコマンドが格納されたパケットを、上記パスＢを介して遠隔保守／操作センタ装置１２０内のサービス装置接続部１２５に送信する。

【００６９】遠隔保守／操作実行部１３４は、該サービス装置接続部１２５から被サービス装置２３０が送信してきた遠隔保守／操作の開始要求依頼のメッセージが格



納されたパケットを受け取ると、被サービス装置２３０の遠隔保守／操作を実行するためのコマンドがデータ部に格納された該被サービス装置２３０宛のパケットを生成し、このパケットを遠隔保守／操作センタ装置１２０のサービス装置１３０に送信するようにセンタ被接続部１３２に依頼する。このパケットは、該センタ被接続部１３２により、コネクションＢを介して遠隔保守／操作センタ装置１２０のサービス装置接続部１２５に送られ、さらに、被サービス装置被接続部１２４によりコネクションＡを介して、被サービス装置２３０に送られる。遠隔保守／操作実行部１３４は、例えば、自社が顧客に販売した装置やソフトウェアなどの障害調査や障害の修正などを遠隔操作により実行する。

【００７０】また、被サービス装置２３０は、センタ接続部２３２、遠隔保守／操作被実行部２３４、及び被サービス装置安全保持部２３５などから構成される。センタ接続部２３２は、自装置２３０の遠隔保守／操作を、契約先のサービス装置１３０に依頼する際に、自社のファイアウォール２２０を介して遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４との間にコネクションＡを確立する。そして、以後、該コネクションＡと前記コネクションＢとで構成される二次パスを介して、サービス装置１３０との間で遠隔保守／操作を実施するためのコマンドや該遠隔保守／操作結果が格納されたパケットの授受を行う。

【００７１】遠隔保守／操作被実行部２３４は、該センタ接続部２３２からサービス装置１３０から送信されてくるパケットを受取り、該パケットから遠隔保守／操作用のコマンドを取り出し、このコマンドを解析・実行する。そして、該コマンドの実行結果、すなわち、遠隔保守／操作の実行結果が格納されたパケットを生成し、このパケットをサービス装置１３０に送信してくれるように、センタ接続部２３２に依頼する。該センタ接続部２３２は、このパケットを上記コネクションＡを介して遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４に送信する。

【００７２】被サービス装置安全保持部２３５は、遠隔保守／操作被実行部２３４からの依頼を受けて、該遠隔保守／操作被実行部２３４がサービス装置１３０から受け取ったパケットのセキュリティ・チェックを行う。すなわち、そのパケットに格納されているコマンドが契約で定められた正当なコマンドであるか否かなどをチェックする。そして、そのチェック結果を遠隔保守／操作被実行部２３４に返す。このセキュリティ・チェックは、例えば、サービス提供者がアクセスしてほしくないファイルを保護するために行われる。

【００７３】被サービス装置２３０は、該被サービス装置安全保持部２３５が上記セキュリティ・チェックを行うためのデータベースとして、非参照ファイル名データベース２３６を備えている。

【００７４】この非参照ファイル名データベース２３６には、顧客がサービス装置１３０に対してアクセスを禁止するファイルの名称が登録されている。上記被サービス装置安全保持部２３５は、サービス装置１３０から送られてくるパケットに格納されているコマンドがこれらのアクセス保護対象のファイルであった場合には、そのコマンドの実行を禁止するように遠隔保守／操作実行部１３４に通知する。

【００７５】これにより、遠隔保守／操作被実行部２３４は、サービス装置１３０から指示されるコマンドの内、自社のセキュリティの安全が保持されるコマンドのみを実行する。

【００７６】次に、上記構成の実施例での動作を、図６を参照しながら説明する。本実施例では、遠隔保守／操作の実行は、顧客側からの要求によって開始される。この要求は、例えば、被サービス装置２３０の表示部に表示されるＧＵＩ（グラフィカル・ユーザ・インターフェース）を介して指示される（Ｓ１１）。

【００７７】この指示がなされると、センタ接続部２３２は、顧客ネットワーク２１０及びファイアウォール２２０を介して、遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４とコネクションＡを確立する。これにより、センタ接続部２３２と被サービス装置被接続部１２４との間にセッションが開設され、これら両部２３２、１２４がコネクションＡを介してパケットを授受することが可能になる。

【００７８】続いて、センタ接続部２３２は、契約時に被サービス装置２３０に割当てられたサービスＩＤ、ユーザＩＤ、被サービス装置ＩＤ、及びパスワードが格納されたパケットを生成し、このパケットを上記コネクションＡを介して、遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４に送信する（Ｓ１２）。

【００７９】被サービス装置被接続部１２４は、上記パケットを受信すると、該パケットに格納されているサービスＩＤ、ユーザＩＤ、被サービス装置ＩＤ、及びパスワードを自社ネットワーク安全保持部１２６に送り、上記パケットが契約ユーザの被サービス装置被接続部１２４から送られてきたものかの判断を依頼する。該自社ネットワーク安全保持部１２６は、上記４種類の情報をユーザ認証用データベース１２１に登録されている情報と照合し、上記パケットが契約ユーザからのものであるか否か判定する。そして、契約ユーザからのパケットであると判定すると（Ｓ１４），上記サービスＩＤをキーとしてサービス装置データベース１２２を検索して、該サービスＩＤに対応するサービス装置１３０を識別し、そのサービス装置１３０のＩＰアドレスを獲得する。そして、該照合結果と共に契約ユーザからのパケットであることが判明した場合には、上記識別したサービス装置１３０のＩＰアドレスも被サービス装置被接続部１２４に返す（Ｓ１５）。

【００８０】一方、上記ステップＳ１４で上記パケットが契約ユーザからのものでないと判断した場合には、このパケットを棄却する。また、上記コネクションＡを切断する。

【００８１】該被サービス装置被接続部１２４は、自社ネットワーク安全保持部１２６から上記判定結果を受け取り、自己が受信したパケットが契約ユーザの被サービス装置２３０から送信されてきたものであると判断すると、上記識別された自社ネットワーク安全保持部１２６に接続されたサービス装置１３０のＩＰアドレスをサービス装置接続部１２５に送り、該サービス装置１３０との間にコネクションＢを確立するように依頼する。サービス装置接続部１２５は、この依頼を受けて、自社ネットワーク１１０を介して上記コネクションＢを、上記サービス装置１３０のセンタ接続部２３２との間に確立する（Ｓ１６）。

【００８２】これにより、サービス装置接続部１２５とセンタ接続部２３２との間にセッションが開設され、これら両部１２５、２３２は、互いにパケットを授受することが可能になる。尚、自社ネットワーク安全保持部１２６が、サービス装置接続部１２５に、直接、上記コネクションＢの確立を依頼するようにしてもよい。

【００８３】続いて、サービス装置接続部１２５は、上記コネクションＢを介して、上記サービス装置１３０のセンタ接続部２３２に被サービス装置２３０との間でパケット通信が可能になったことを通知する（Ｓ１７）。

【００８４】該センタ接続部２３２は、この通知を受けて、遠隔保守／操作実行部１３４に被サービス装置２３０に対する遠隔保守／操作の実行を開始するように要求する。遠隔保守／操作実行部１３４は、この要求を受け取ると、予め、契約時に定められた遠隔保守／操作の実施を開始する。この実施は、該遠隔保守／操作実行用のコマンドが格納されたパケットを契約先の被サービス装置２３０に送信することによって実行される。すなわち、遠隔保守／操作実行部１３４は、このパケットを生成し、これを上記被サービス装置２３０に送信してくれるようにセンタ被接続部１３２センタに依頼する（Ｓ１８）。

【００８５】該センタ被接続部１３２は、上記依頼を受けると、該遠隔保守／操作実行用のパケットを、コネクションＢを介して遠隔保守／操作センタ装置１２０のサービス装置接続部１２５に送信する（Ｓ１９）。

【００８６】該サービス装置接続部１２５は、上記遠隔保守／操作実行用のパケットを受け取ると、このパケットをコネクションＡを介して被サービス装置２３０のセンタ被接続部１３２に送信する（Ｓ２０）。

【００８７】該センタ被接続部１３２は、上記遠隔保守／操作実行用のパケットを受信すると、このパケットの正当性のチェックを被サービス装置安全保持部２３５に依頼する。そして、被サービス装置安全保持部２３５か

ら、該パケットに格納されている遠隔保守／操作実行用のコマンドが正しいものであるとの判定結果を受け取ると、該コマンドの実行を遠隔保守／操作実行部１３４に依頼する。該遠隔保守／操作実行部１３４は、該コマンドを実行し、その実行結果が格納されたパケットを生成し、このパケットをサービス装置１３０に送信してくれるように、センタ被接続部１３２に依頼する。該センタ被接続部１３２は、受け取ったパケットをコネクションＡを介して遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４に送信する（Ｓ２１）。

【００８８】尚、このとき、被サービス装置安全保持部２３５によって、上記サービス装置１３０が指示するコマンドが非参照ファイル名データベース２３６に登録されているファイルをアクセスするコマンドであると判定されたならば、遠隔保守／操作実行部１３４は該コマンドを実行しない（Ｓ２２）。

【００８９】該被サービス装置被接続部１２４は、該遠隔保守／操作の実行結果が格納されたパケットを受信すると、このパケットをコネクションＢを介してサービス装置１３０のセンタ被接続部１３２に送信する（Ｓ２３）。

【００９０】該センタ被接続部１３２は、上記パケットを受信すると、該パケットから上記遠隔保守／操作の実行結果を取り出し、これを遠隔保守／操作実行部１３４に送る。該遠隔保守／操作実行部１３４は、該実行結果を自装置１３０の表示部に画面表示する（Ｓ２４）。

【００９１】上記ステップＳ１８～Ｓ２４の処理は、被サービス装置２３０で遠隔保守／操作の実行が指示される間、繰り返される。尚、この遠隔保守／操作の実行指示は、例えば、サービス装置１３０の表示の画面に表示されるＧＵＩ（グラフィカル・ユーザ・インターファエイス）を介しておこなわれる。

【００９２】遠隔保守／操作実行部１３４は、被サービス装置２３０に対する全ての遠隔保守／操作の実行を終了すると、センタ被接続部１３２に遠隔保守／操作の実施が終了した旨をセンタ被接続部１３２に通知する（Ｓ２５）。

【００９３】該センタ被接続部１３２は、この通知を受けて上記コネクションＢの切断処理を実行する（Ｓ２６）。遠隔保守／操作センタ装置１２０のサービス装置接続部１２５は、上記コネクションＢの切断処理が終了すると、新しいパスワードを被サービス装置２３０に送付するためのパケットを生成し、このパケットをコネクションＡを介して、被サービス装置２３０のセンタ被接続部１３２に送信する。遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４は、被サービス装置２３０からその新しいパスワードの受信の確認を受け取ると、コネクションＡを切断する処理を行う（Ｓ２７）。

【００９４】被サービス装置２３０は、上記コネクションＡの切断処理が終了した後、この新しいパスワードを、次回の遠隔保守／操作のために使用するために所定の記憶装置に記憶する（Ｓ２８）。

【００９５】次に、上記遠隔保守／操作の実行時におけるパケットの流れを、詳細に説明する。ここでは、図７に示すように自社ネットワーク１１０と顧客ネットワーク２１０が互いにインターネット２５０によって接続され、自社ネットワーク１１０内の遠隔保守／操作センタ装置１２０とサービス装置１３０、及び顧客ネットワーク２１０のファイアウォール２２０と被サービス装置２３０に対して、同図に示すようなＩＰアドレスとポート番号が割当られているものとして説明する。

【００９６】すなわち、自社ネットワーク１１０においては、遠隔保守／操作センタ装置１２０のＩＰアドレスは”Ｃ”に、その被サービス装置被接続部１２４のポート番号は”Ｐ１”に設定されている。また、サービス装置１３０のＩＰアドレスは、”Ｄ”に設定されている。

【００９７】一方、顧客ネットワーク２１０においては、被サービス装置２３０のＩＰアドレスは”Ａ”に、そのセンタ被接続部１３２のポート番号は”Ｐ２”に設定されている。また、ファイアウォール２２０のＩＰアドレスは”Ｂ”に設定されている。

【００９８】次に、図８は、自社ネットワーク１１０と顧客ネットワーク２１０間で授受されるパケット内のＩＰデータグラムに設定されるヘッダ部３００の構成を示す図である。

【００９９】上記ヘッダ部３００は、ＩＰヘッダ３０１とＴＣＰヘッダ３０２に加え、遠隔保守／操作ヘッダとから構成される。ＩＰヘッダ３０１には、発信ＩＰアドレス（ソースアドレス）、受信ＩＰアドレス（デスティネーションアドレス）などＩＰプロトコルによって定められている各種情報が設定される。また、ＴＣＰヘッダ３０２には、発信ポート番号（ソースポート番号）、受信ポート番号（デスティネーションポート番号）、ＳＥＱ（Ｓｅｑｅｎｃｅ　Ｎｕｍｂｅｒ）などＴＣＰプロトコルによって定められている各種情報が設定される。

【０１００】また、遠隔保守／操作ヘッダ３０３は、本実施例の特徴となるもので、前述したように、被サービス装置被接続部１２４がコネクションＡを介して受信するパケットが、契約先のユーザからのものであるか否かを判定するためのセキュリティ・チェックに用いられるサービスＩＤ（ＳＶＩＤ）、ユーザＩＤ（ＵＩＤ）、パスワード（ＰＷＤ）、及び被サービス装置ＩＤ（ＷＩＤ）が設定される。この遠隔保守／操作ヘッダ３０３は、上記ＴＣＰヘッダ３０２のデータ部に設定される。

【０１０１】図９～図１１は、図６のフローチャートで説明した処理におけるパケットの流れとそのパケットの内容を説明する図である。ここで、図１２に、被サービス装置２３０とサービス装置１３０間で送受信されるパケット４００のフォーマットを示す。このパケット４０

0は、通常のＩＰデータグラムのＴＣＰ／ＩＰヘッダ４００ａの後に、上記被サービス装置２３０とサービス装置１３０との間で遠隔保守／操作を実施するために用いる遠隔保守／操作ヘッダ４００ｂと通知情報などのデータ４００ｃが設定される。上記ＴＣＰ／ＩＰヘッダ４００ａは、前記図８に示すＩＰヘッダ３０１とＴＣＰヘッダ３０２とから構成され、また、上記遠隔保守／操作ヘッダ４００ｂの内容は、図８に示す遠隔保守／操作ヘッダ３０３のようになっている。

【０１０２】また、図９～図１１に示すパケット４０１～４０６の内、被サービス装置２３０からサービス装置１３０に送信されるパケット４０１～４０３のＴＣＰ／ＩＰヘッダの形式は図１３（ａ）に示すとうりである。また、サービス装置１３０から被サービス装置２３０に送信されるパケット４０４～４０６のＴＣＰ／ＩＰヘッダの形式は図１３（ｂ）に示すとうりである。

【０１０３】図９から図１１に示す被サービス装置２３０とサービス装置１３０との間でのパケット（ＩＰデータグラム）の通信では、被サービス装置２３０と遠隔保守／操作センタ装置１２０間に確立されるコネクション（セッション）Ａと遠隔保守／操作センタ装置１２０とサービス装置１３０間に確立されるコネクション（セッション）Ｂが利用される。

【０１０４】顧客ネットワーク２１０の被サービス装置２３０のセンタ接続部２３２は、コネクションＡを確立した後、図１３に示すＴＣＰヘッダのデータ部に遠隔保守／操作ヘッダが格納されたパケット（ＩＰデータグラム）４０１をファイアウォール２２０に送信する。該ファイアウォール２２０は、このパケット４０１を顧客ネットワーク２１０を介して受信すると、ＩＰヘッダの発信ＩＰアドレスを、被サービス装置２３０のＩＰアドレスである”Ａ”から自己のＩＰアドレスである”Ｂ”に置き換える。そして、この発信ＩＰアドレスの置き換えが行われたパケット（ＩＰデータグラム）４０２をインターネット２５０を介して顧客ネットワーク２１０の遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４に送信する。

【０１０５】以上のパケットの通信はコネクション（セッション）Ａを用いて行われる。このとき、自社ネットワーク１１０の遠隔保守／操作センタ装置１２０が受信するパケット４０２の発信ＩＰアドレスには、顧客ネットワーク２１０に設置されたファイアウォール２２０のＩＰアドレス”Ｂ”が設定されているので、自社ネットワーク１１０は、被サービス装置２３０のＩＰアドレス”Ａ”を知ることはできない。

【０１０６】遠隔保守／操作センタ装置１２０は、上記パケット４０２を受信すると顧客ネットワーク２１０側のファイアウォール２２０とのセッションＡを維持したまま、該パケット４０２の遠隔保守／操作ヘッダを調べる。すなわち、自社ネットワーク安全保持部１２６が、



該遠隔保守／操作ヘッダに設定されている、サービスＩＤ、ユーザＩＤ、パスワード、及び被サービス装置ＩＤがユーザ認証用データベース１２１に登録されているか否か調べる。そして、該登録が確認されたならば、上記サービスＩＤを基に、サービス装置データベース１２２からそのサービスＩＤを有するサービス装置１３０のＩＰアドレス（この場合、”Ｄ”）を取り出す。サービス装置接続部１２５は、このＩＰアドレス”Ｄ”を自社ネットワーク安全保持部１２６から受け取り、サービス装置１３０のセンタ被接続部１３２との間にコネクション（セッション）Ｂを確立する。

【０１０７】続いて、センタ被接続部１３２は、図１０に示すパケット（ＩＰデータグラム）４０３を生成する。すなわち、該パケット４０３の受信ＩＰアドレスに”Ｄ”を設定すると共に、発信ＩＰアドレスに自己のＩＰアドレス”Ｃ”を設定する。また、このパケット４０３の受信ポート番号にサービス装置１３０のセンタ接続部２３２に割り当てられるポート番号（この場合、”Ｐ３”）を設定する。また、ＴＣＰヘッダのデータ部分に、ユーザからのセッション要求の通知情報を設定する。そして、サービス装置接続部１２５は、このパケット４０３を自社ネットワーク１１０を介してサービス装置１３０のセンタ被接続部１３２に送信する。

【０１０８】サービス装置１３０では、上記パケット４０３をセンタ被接続部１３２により受信すると、遠隔保守／操作実行部１３４が該パケット４０３のデータ部に格納されているユーザ（サービス提供者）からの指示データを解釈する。そして、該指示データによって指示されている保守／操作を実行するためのコマンド（サービス提供者への指示情報）を作成し、このコマンドがデータ部にセットされたパケット（ＩＰデータグラム）４０４を生成する。また、この場合、パケット４０４の受信ＩＰアドレスに遠隔保守／操作センタ装置１２０のＩＰアドレス”Ａ”を、送信ＩＰアドレスにサービス装置１３０のＩＰアドレス”Ｄ”を設定する。さらに、受信ポート番号に遠隔保守／操作センタ装置１２０のサービス装置接続部１２５のポート番号”Ｐ３”を、送信ポート番号にセンタ被接続部１３２のポート番号”Ｐ３”を設定する。そして、センタ被接続部１３２は、このパケット４０４をコネクションＢを介して遠隔保守／操作センタ装置１２０のサービス装置接続部１２５に送信する。

【０１０９】遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４は、このパケット４０４をサービス装置接続部１２５から受け取ると、図１０に示すパケット（ＩＰデータグラム）４０５を生成する。サービス装置接続部１２５は、パケット４０４の受信ＩＰアドレス、発信ＩＰアドレス、及び受信ポート番号を変換する。すなわち、パケット４０５の受信ＩＰアドレスに顧客ネットワーク２１０のファイアウォール２２０のＩＰアドレス”Ｂ”を、発信ＩＰアドレスに自装置１２０の

ＩＰアドレス”Ｃ”を設定する。さらに、受信ポート番号に顧客ネットワーク２１０に接続された被サービス装置２３０のセンタ被接続部１３２のポート番号”Ｐ２”を設定する。そして、被サービス装置被接続部１２４は、コネクションＡを介してこのパケット４０５を顧客ネットワーク２１０のファイアウォール２２０に送信する。　ファイアウォール２２０は、該パケット４０５を受信すると、まず、ＩＰアドレスの変換処理を行い、図１１に示すパケット（ＩＰデータグラム）４０６を生成する。すなわち、受信ＩＰアドレスを”Ｂ”から被サービス装置２３０のＩＰアドレス”Ａ”に、発信ＩＰアドレスを”Ｃ”から自己のＩＰアドレス”Ｂ”に変換する。そして、ファイアウォール２２０は、被サービス装置２３０からのセッションを利用してパケット４０６を被サービス装置２３０のセンタ接続部２３２に送信する。

【０１１０】このように、被サービス装置２３０は、発信ＩＰアドレスがファイアウォール２２０のＩＰアドレスのパケットのみを受信する。したがって、サービス装置１３０のＩＰアドレスを知ることはできない。

【０１１１】センタ接続部２３２は、該パケット４０６を受信すると、これを遠隔保守／操作実行部１３４に送る。遠隔保守／操作実行部１３４は、該パケット４０６からサービス提供者の指示情報を取り出し、これを解釈して、その指示情報によって指示されている保守／操作を実行する。尚、この保守／操作の実行の前に被サービス装置安全保持部２３５によって、上記サービス提供者の指示情報が正当であるか否かのチェックが行われる。そして、遠隔保守／操作実行部１３４は、このチェックにより正当であると判定された指示情報のみを実行する。

【０１１２】遠隔保守／操作実行部１３４は、上記遠隔保守／操作の実行が終了すると、その実行結果がＴＣＰヘッダのデータ部に格納されたパケット（ＩＰデータグラム）を生成する。このパケットは、以上、説明した、コネクションＡ及びコネクションＢにより結ばれた二次パス（図５参照）を逆方向に経由して、自社ネットワーク１１０に接続されたサービス装置１３０に送られる。

【０１１３】次に、遠隔保守／操作センタ装置１２０が、顧客ネットワーク２１０に設置されたファイアウォール２２０を介して、該顧客ネットワーク２１０に接続された被サービス装置２３０とコネクション（セッション）Ａを確立する動作を、より詳細に説明する。

【０１１４】図１４は、遠隔保守／操作センタ装置１２０が被サービス装置２３０とサービス装置１３０との間のパケット（ＩＰデータグラム）の中継処理を実行する動作を説明するフローチャートである。遠隔保守／操作センタ装置１２０が被サービス装置２３０とサービス装置１３０との間のパケット（ＩＰデータグラム）の中継処理を実行する動作を説明するフローチャートである。



【０１１５】ところで、顧客ネットワーク２１０に設置されたファイアウォール２２０は、例えば、ＴＣＰポートフィルタリング機能を備えており、遠隔保守／操作の契約が成立すると、遠隔保守／操作を提供する業者は、遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４に割当てられているポート番号を、契約先のユーザに通知する。これを受けて、契約先のファイアウォール２２０の管理者は、顧客ネットワーク２１０に接続された自社の被サービス装置２３０と遠隔保守／操作センタ装置１２０の被サービス装置被接続部１２４が互いにパケットをファイアウォール２２０を介して送受信できるように、ファイアウォール２２０のＴＣＰポートフィルタリングを設定する。尚、上記被サービス装置被接続部１２４のポート番号は、固定であってもよく、また、各被サービス装置２３０ごとに個別のポート番号を割当てるようにしてもよい。

【０１１６】また、顧客ネットワーク２１０に設置されたファイアウォール２２０がＩＰアドレスフィルタリング機能を備えている場合には、遠隔保守／操作を提供する業者は、遠隔保守／操作センタ装置１２０のＩＰアドレスを契約先のユーザに知らせ、該遠隔保守／操作センタ装置１２０が被サービス装置２３０宛に送信するパケットがファイアウォール２２０を通過できるようにＩＰアドレスフィルタを設定してもらうようにお願いする。

【０１１７】被サービス装置被接続部１２４は、常時、被サービス装置２３０からのセッション（コネクション）確立要求待ちにある（Ｓ４１）。そして、被サービス装置被接続部１２４は、ファイアウォール２２０を介して被サービス装置２３０が送信してきたセッション確立要求のメッセージが格納されたパケットを受け取ると、そのパケットの遠隔保守／操作ヘッダに設定されているサービスＩＤ、ユーザＩＤ、パスワード、及び被サービス装置ＩＤがユーザ認証用データベース１２１に登録されているか否かのチェックを、自社ネットワーク安全保持部１２６に依頼する（Ｓ４２）。

【０１１８】続いて、被サービス装置被接続部１２４は、自社ネットワーク安全保持部１２６からそのチェック結果を受取り、被サービス装置２３０が契約されたユーザのものであるか否かを判別する（Ｓ４３）。

【０１１９】次に、被サービス装置被接続部１２４は、上記チェック結果により、セッション確立要求のパケットが契約先の被サービス装置２３０からのものでないと判別すると（Ｓ４３，ＮＧ），このセッション（コネクション）確立要求を棄却（リジェクト）する（Ｓ４４）。

【０１２０】一方、被サービス装置被接続部１２４は、セッション確立要求のパケットが契約先の被サービス装置２３０からのものであると判別すると（Ｓ４３，ＯＫ），サービス装置接続部１２５に上記パケットに格納されているサービスＩＤを送る。サービス装置接続部１

２５は、このサービスＩＤを受け取ると、このサービスＩＤに対応するサービス装置１３０のＩＰアドレスを、サービス装置データベース１２２を検索して、読みだす（Ｓ４５）。

【０１２１】そして、サービス装置接続部１２５は、このＩＰアドレスを用いて、自社ネットワーク１１０を介して該ＩＰアドレスを有するサービス装置１３０とセッション（コネクション）Ｂを確立する（Ｓ４６）。

【０１２２】次に、サービス装置接続部１２５は、被サービス装置２３０とサービス装置１３０とのセッション（コネクション）を維持したままで、この新たにセッションが確立された被サービス装置２３０用の子プロセスを生成する（Ｓ４７）。

【０１２３】続いて、サービス装置接続部１２５は、別の被サービス装置２３０からのセッヨン要求を待つシステム・コールを行い（Ｓ４８）、上記ステップＳ４１に戻る。

【０１２４】以上述べたステップＳ４１～Ｓ４８の処理により、遠隔保守／操作センタ装置１２０により、被サービス装置２３０とサービス装置１３０との間には複数のセッションが確立される。すなわち、サービス装置１３０は複数の被サービス装置２３０に対して遠隔保守／操作のサービスを実施することができる。

【０１２５】図１４には、被サービス装置Ａ，Ｂ，及びＣの３台の被サービス装置２３０とサービス装置１３０との間に確立されたセッションによって生成された子プロセスが示されている。各子プロセスは、被サービス装置２３０用のバッファ１２７（１２７Ａ，１２７Ｂ，１２７Ｃ）とサービス装置１３０用のバッファ１２８（１２８Ａ，１２８Ｂ，１２８Ｃ）を備える。被サービス装置２３０からサービス装置１３０に対してパケットが送信される場合には、このパケットは、いったん被サービス装置被接続部１２４によって被サービス装置２３０用のバッファ１２７に格納された後、該バッファ１２７からサービス装置１３０用のバッファ１２８にコピーされる。そして、このバッファ１２８に格納されたパケットは、サービス装置接続部１２５によって取り出され、該サービス装置接続部１２５によって当該サービス装置１３０に送出される。

【０１２６】また、図１４には示していないが、サービス装置１３０から被サービス装置２３０に対してパケットが送信される場合には、このパケットは、いったんサービス装置接続部１２５によってサービス装置１３０用のバッファ１２８に格納された後、該バッファ１２８から被サービス装置２３０用のバッファ１２８にコピーされる。そして、このバッファ１２７に格納されたパケットは、被サービス装置被接続部１２４によって取り出され、該被サービス装置被接続部１２４によって当該被サービス装置２３０に送出される。

【０１２７】以上のようにして、コネクションＡとコネクションＢの２つのコネクションを用いることにより、遠隔保守／操作センタ装置１２０を介して、被サービス装置２３０とサービス装置１３０との間でパケット（ＩＰデータグラム）の授受が行われ、該サービス装置１３０によって、該被サービス装置２３０の遠隔保守／操作が実施される。

【０１２８】次に、図１５は、遠隔保守／操作センタ装置１２０のＩＰ中継機能を別の観点から説明するフローチャートである。同図において、前記図１４で説明したステップと同一のステップＳ４１～Ｓ４６によって、被サービス装置２３０からのセッション確立要求によって、サービス装置接続部１２５が自社ネットワーク１１０を介してサービス装置１３０との間にセッション（コネクションＢ）を確立する。

【０１２９】該サービス装置接続部１２５は、上記セッションを確立すると、セッション管理テーブルを作成する（Ｓ５１）。このセッション管理テーブルは、（セッション番号、被サービス装置セッションＩＤ，サービス装置セッションＩＤ）の３種類の情報から成る。被サービス装置セッションＩＤは、被サービス装置２３０と被サービス装置被接続部１２４との間に確立されるコネクションＡによって開設されるセッションに関するものである。また、サービス装置セッションＩＤは、サービス装置接続部１２５と被サービス装置２３０との間に確立されるコネクションＢによって開設されるセッションに関するものである。この被サービス装置セッションＩＤとサービス装置セッションＩＤによって、被サービス装置２３０とサービス装置１３０との間に確立される一本の論理パスに関する情報が得られ、遠隔保守／操作センタ装置１２０は、被サービス装置２３０とサービス装置１３０との間で授受されるパケット（ＩＰデータグラム）の中継処理を実行できる。尚、上記セッションＩＤは、サービス装置接続部１２５がＴＣＰプロトコル層で管理しているもので、発信ＩＰアドレス、受信ＩＰアドレス、発信ポート番号、受信ポート番号などの情報により区別される各個別のセッション（コネクション）を識別するためのＩＤである。セッション管理テーブルにおいては、一組の被サービス装置セッションＩＤとサービス装置セッションＩＤによって定まる被サービス装置２３０とサービス装置１３０との間の各セッションについて、一意のセッション番号が割当てられる。

【０１３０】続いて、遠隔保守／操作センタ装置１２０（被サービス装置被接続部１２４またはサービス装置接続部１２５）は、各装置（被サービス装置２３０またはサービス装置１３０）から送信されてくるパケットの入力待ちとなる（Ｓ５２）。

【０１３１】そして、遠隔保守／操作センタ装置１２０（被サービス装置被接続部１２４またはサービス装置接続部１２５）は、各装置（被サービス装置２３０またはサービス装置１３０）からパケットを入力すると、前記

セッション管理テーブルを検索して、上記入力されたパケットが送信されてきたセッションのＩＤ（セッションＩＤ）を基に、セッション管理テーブルを検索して（Ｓ５３），該セッション管理テーブルから上記セッションＩＤに対応する装置（被サービス装置２３０またはサービス装置１３０）のセッションＩＤを取り出す（Ｓ５４）。すなわち、被サービス装置２３０からのパケットを被サービス装置被接続部１２４が受信した場合には、該被サービス装置被接続部１２４は、そのパケットが送られてきたセッション（被サービス装置セッションＩＤ）に対応するサービス装置セッションＩＤを取り出す。一方、サービス装置１３０からのパケットをサービス装置接続部１２５が受信した場合には、該サービス装置接続部１２５は、そのパケットが送られてきたセッション（サービス装置セッションＩＤ）に対応する被サービス装置２３０サービス装置セッションＩＤを取り出す。

【０１３２】そして、サービス装置接続部１２５は、上記取り出したセッションＩＤを基に、被サービス装置２３０から送信されてきたパケットを、当該サービス装置１３０に送出する。また、被サービス装置被接続部１２４は、上記取り出したセッションＩＤを基に、サービス装置１３０から送信されてきたパケットを、当該被サービス装置２３０に送出する（Ｓ５５）。

【０１３３】以上、述べたように、本実施例によれば、遠隔保守／操作サービスを提供する業者の内部ネットワークと該業者から遠隔保守／操作のサービスを受ける装置を有する顧客のネットワークが、インターネットや公衆回線などの外部ネットワークによって互いに接続され、かつ、両社が該外部ネットワークに対してファイアウォールを設置しているシステム形態において、遠隔保守／操作サービス提供業者は内部ネットワークに接続されているサービス装置を用いて、顧客側の内部ネットワークに接続されている被サービス装置を、遠隔保守／操作することができる。しかも、この場合、互いにセキュリティ・ガード機構を備えているので、両者とも内部ネットワークの安全性を保持することができる。

【０１３４】また、本実施例では、上記外部ネットワークとして商用インターネットを利用することが可能である。この場合、ダイアル・アップＩＰ接続のユーザも顧客の対象にすることができる。また、この場合、商用インターネットとの回線接続時にＩＰアドレスが割当てられる端末型のダイアル・アップＩＰ接続を利用するユーザも顧客の対象にすることができる。すなわち、本実施例では、受信したパケットが契約先のユーザからのものであるか否かを、契約時に登録されるサービスＩＤ、ユーザＩＤ、被サービス装置ＩＤ、及びパスワードにより認証するので、ＩＰアドレスのみに頼らずに、契約ユーザの認証を行うことが可能だからである。

【０１３５】尚、上記実施例では、ＴＣＰ／ＩＰプロトコルを利用して遠隔保守／操作を実施するためのパケットの送受信を行うようにしているが、本発明は、プロトコルが限定されるものではなく、その他のプロトコルを採用することも可能である。また、契約先のユーザと遠隔保守／操作の提供業者のそれぞれの社内ネットワークは、必ずしも、インターネットで接続されている必要はなく、その他のコモン・キャリアによって提供される各種のネットワークで接続されていてもよい。また、遠隔保守／操作のみならず、広い意味での遠隔操作全般に適用可能なものである。



【０１３６】

【発明の効果】本発明によれば、遠隔操作サービスを受ける顧客と該サービスを実施する業者が、外部ネットワークにファイアウォールを設置したままで、それぞれの社内ネットワークに接続された装置により、遠隔操作を実施できる。したがって、既存の社内ネットワークをそのまま利用して、安全で安価な遠隔操作サービスシステムを実現できる。

【０１３７】また、被サービス装置には、契約事項以外の遠隔操作の実行を阻止するセキュリティ・チェック機構が設けられるので、安全性は保証される。一方、遠隔操作実施業者でも、契約ユーザの被サービス装置とコネクションを確立した後に、該コネクションを介して送られてくるパケットに正式な契約ユーザであることを示す認証情報が設定されているか否かをチェックするセキュリティ・チェック機構を設けているので、サービス装置に対する不正なアクセスを防止できる。

【図面の簡単な説明】

【図１】本発明の原理を説明する図（その１）である。

【図２】本発明の原理を説明する図（その２）である。

【図３】本発明の原理を説明する図（その３）である。

【図４】本発明の原理を説明する図（その４）である。

【図５】本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図である。

【図６】上記実施例の全体動作を説明する図である。

【図７】上記実施例の一つのシステム形態例を示す図である。

【図８】図７に示すシステムにおいて、自社ネットワークと顧客ネットワーク間で授受されるパケット内のＩＰデータグラムに設定されるヘッダ部の構成を示す図である。

【図９】図７に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その１）である。

【図１０】図７に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その２）である。

【図１１】図７に示すシステムでサービス装置が顧客の

31

被サービス装置の遠隔保守／操作を実施する際に、上記両装置間で授受されるパケットの内容を示す図（その３）である。

【図１２】上記図９～図１１に示す動作中において、被サービス装置とサービス装置間で送受信されるパケットのフォーマットを示す図である。

【図１３】上記図９及び図１１に示されたパケットのフォーマットを説明する図である。

【図１４】遠隔保守／操作センタ装置が被サービス装置とサービス装置との間のパケット（ＩＰデータグラム）の中継処理を実行する動作を説明するフローチャートである。

【図１５】上記図１４のフローチャートに示された遠隔保守／操作センタ装置１２０のＩＰ中継機能を別の観点から説明するフローチャートである。

【図１６】ファイアウォールのパケットフィルタリングゲートウェイ機能を説明する図である。

【図１７】ファイアウォールの第二の機能であるＩＰアドレス変換／中継機能を説明する図である。

【図１８】Ａ社、Ｂ社、Ｃ社、及びＤ社の内部ネットワークがファイアウォールを介して、商用インターネットに接続されたシステムを示す図である。

32

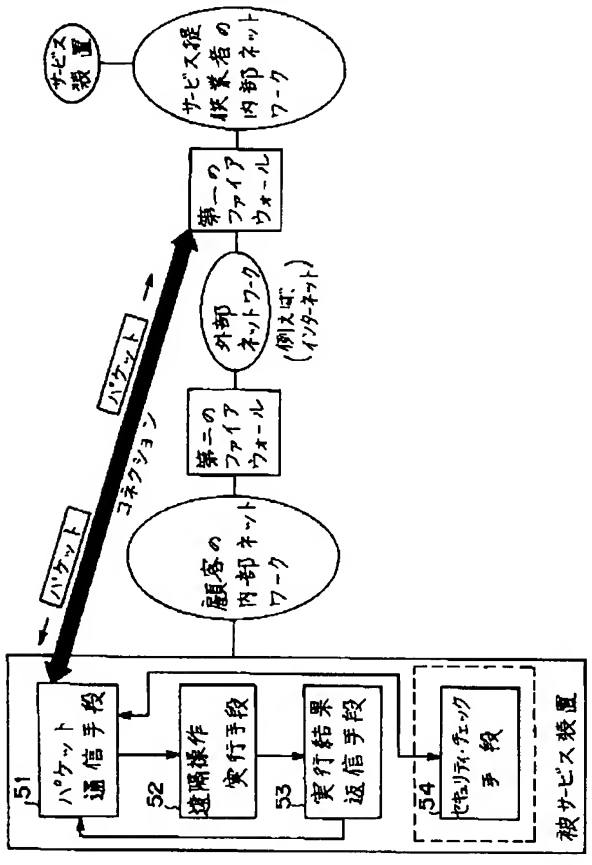
【図１９】上記図１８に示すシステムにおいて、Ａ社の内部ネットワークに接続されたサービス装置がＤ社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施できない原因を説明する図である。

【図２０】上記図１８に示すシステムにおいて、Ａ社の内部ネットワークに接続されたサービス装置がＤ社の内部ネットワークに接続された被サービス装置を遠隔保守／操作を実施する従来の方法を説明する図である。

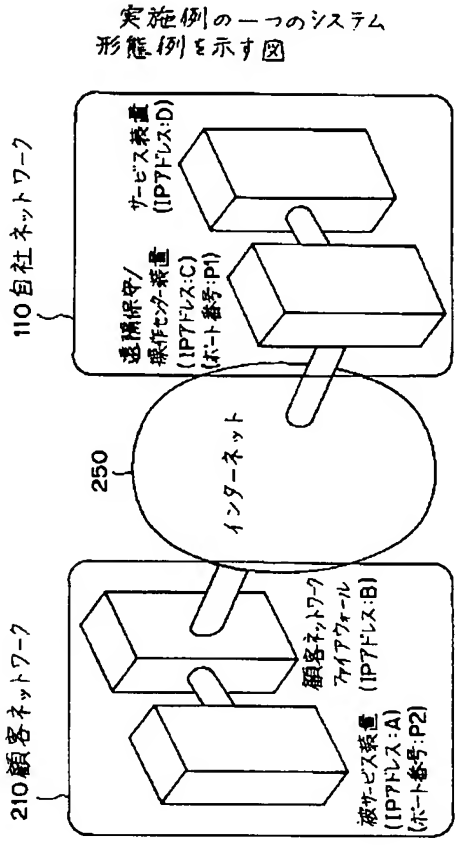
【符号の説明】

| | |
|---|---|
| ５１、７１ | パケット通信手段 |
| ５２、７２ | 遠隔操作実行手段 |
| ５３ | 実行結果返信手段 |
| ５４、６２ | セキュリティ・チェック手段 |
| ６１ | 第一のパケット通信手段 |
| ６３ | 第二のパケット通信手段 |
| ８１ | 被サービス装置 |
| ８２ | 顧客の内部ネットワーク |
| ８３ | 第一のファイアウォール |
| ８４ | 外部ネットワーク |
| ８５ | 第二のファイアウォール |
| ８６ | サービス提供業者の内部ネットワーク |
| ８７ | サービス装置 |

【図１】

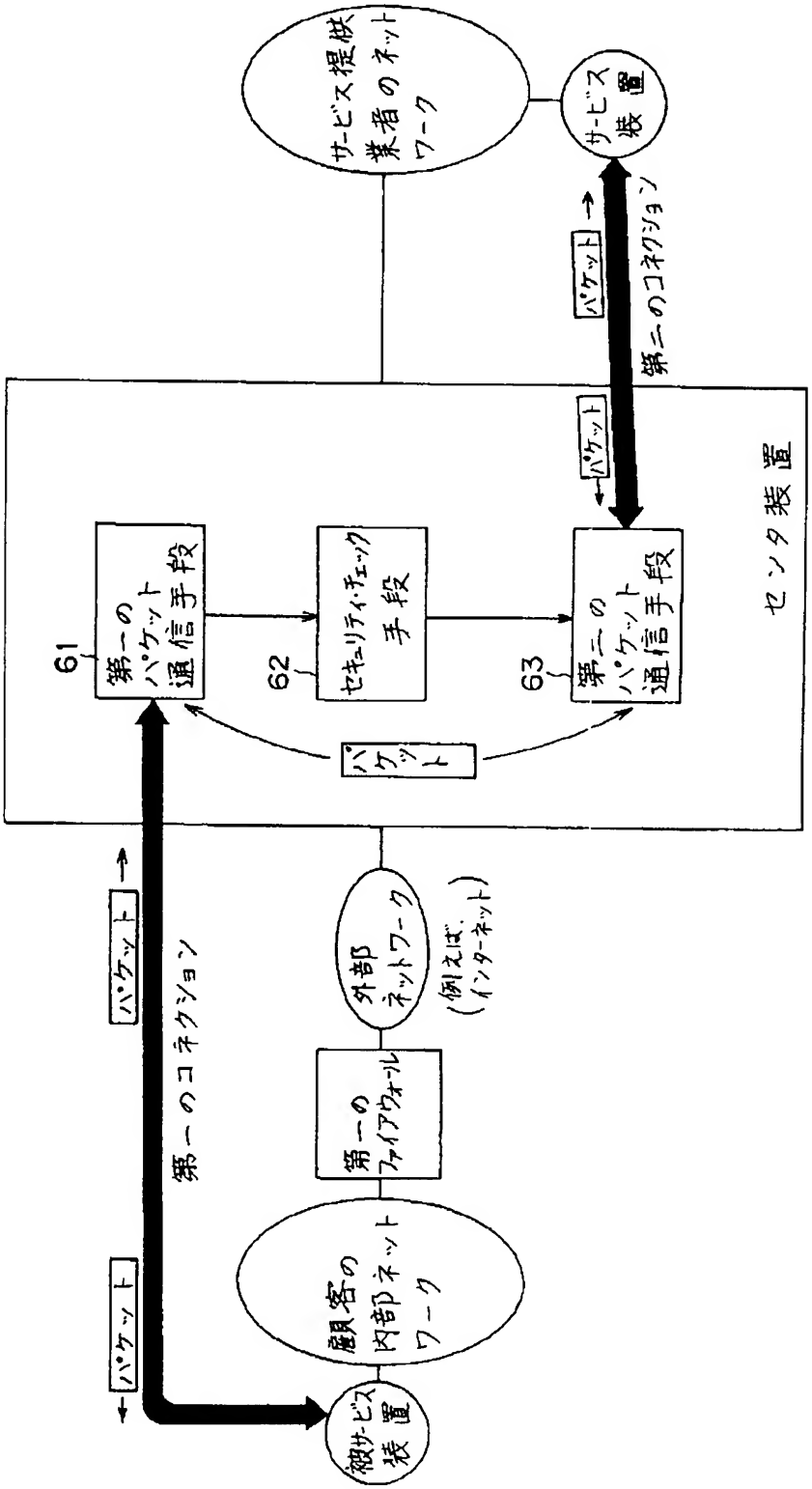



【図７】



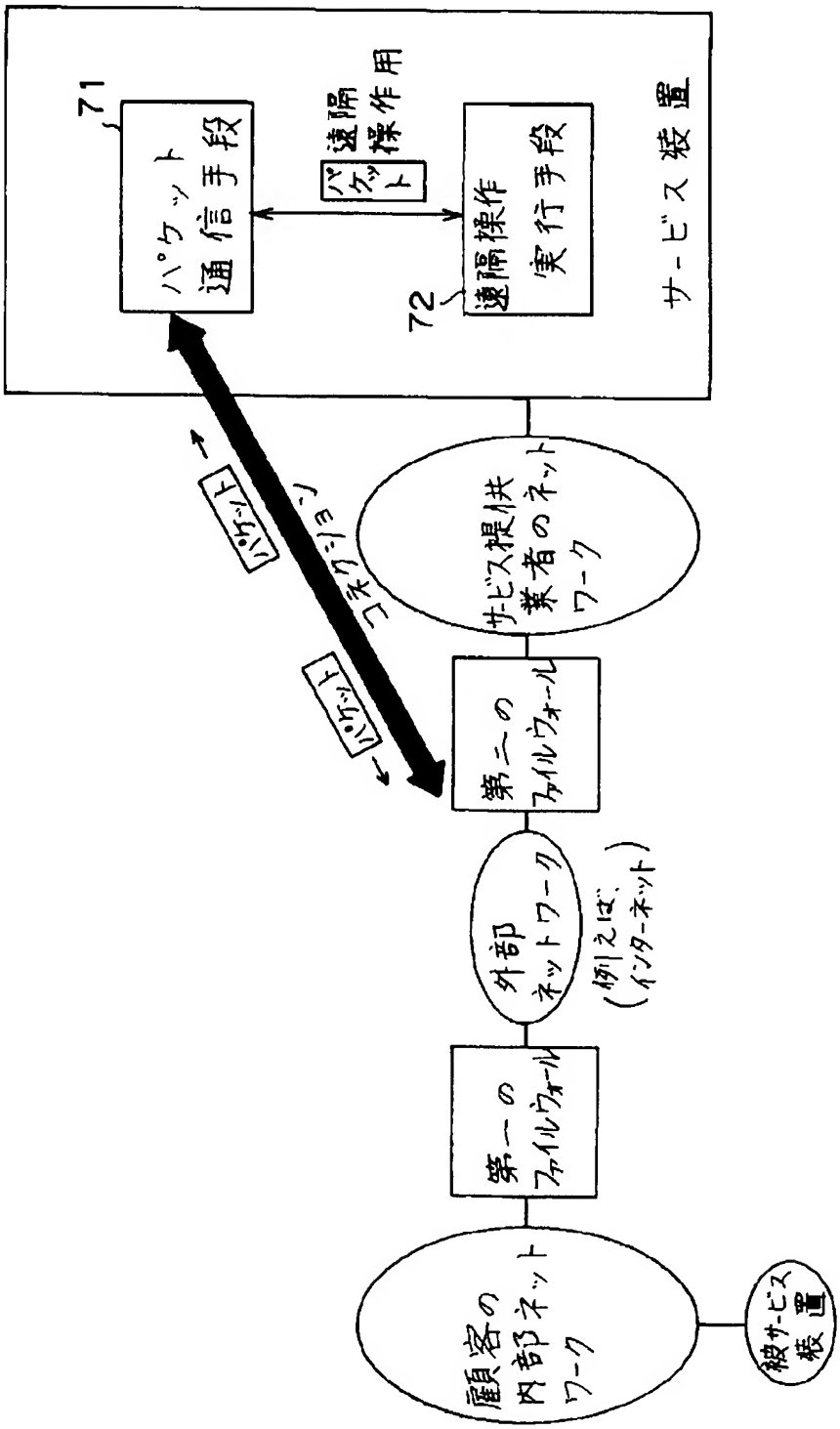
【図2】

本発明の原理を説明する図（その2）



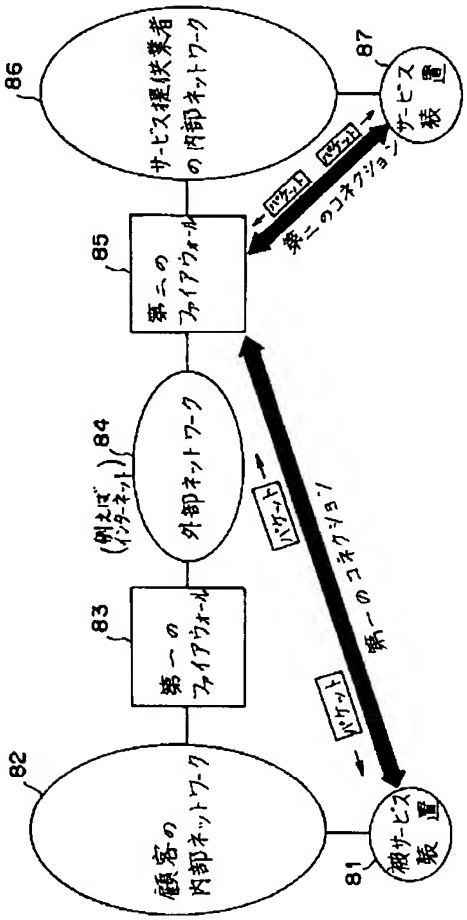
【図3】

本発明の原理を説明する図（その3）



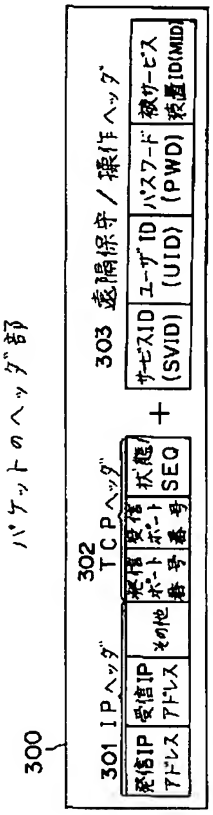
【図4】

本発明の原理を説明する図（その4）



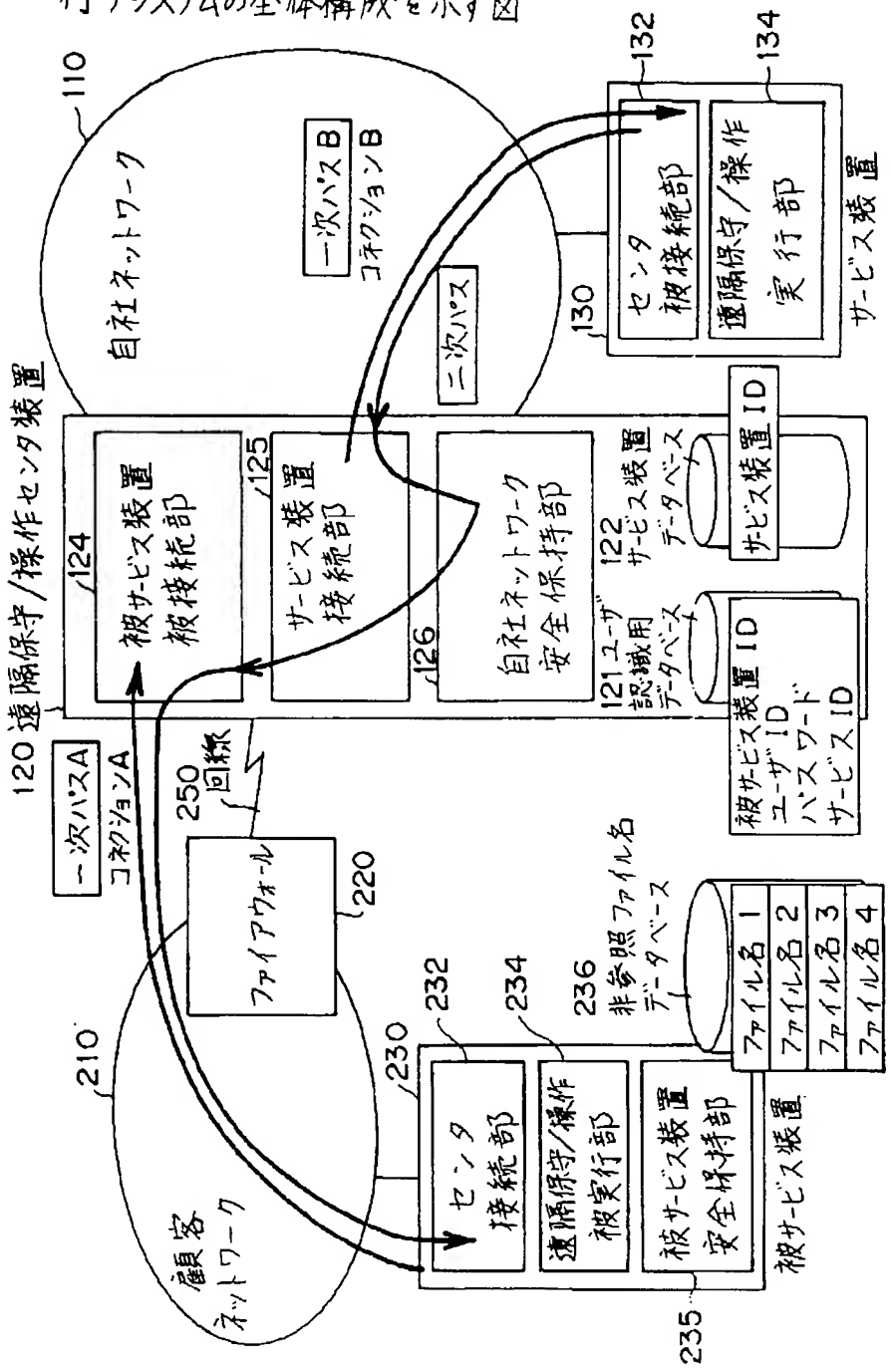

【図8】

図7に示すシステムにおいて、自社ネットワークと顧客ネットワーク間で授受されるパケット内のIPデータグラムに設定されるヘッダ部の構成を示す図

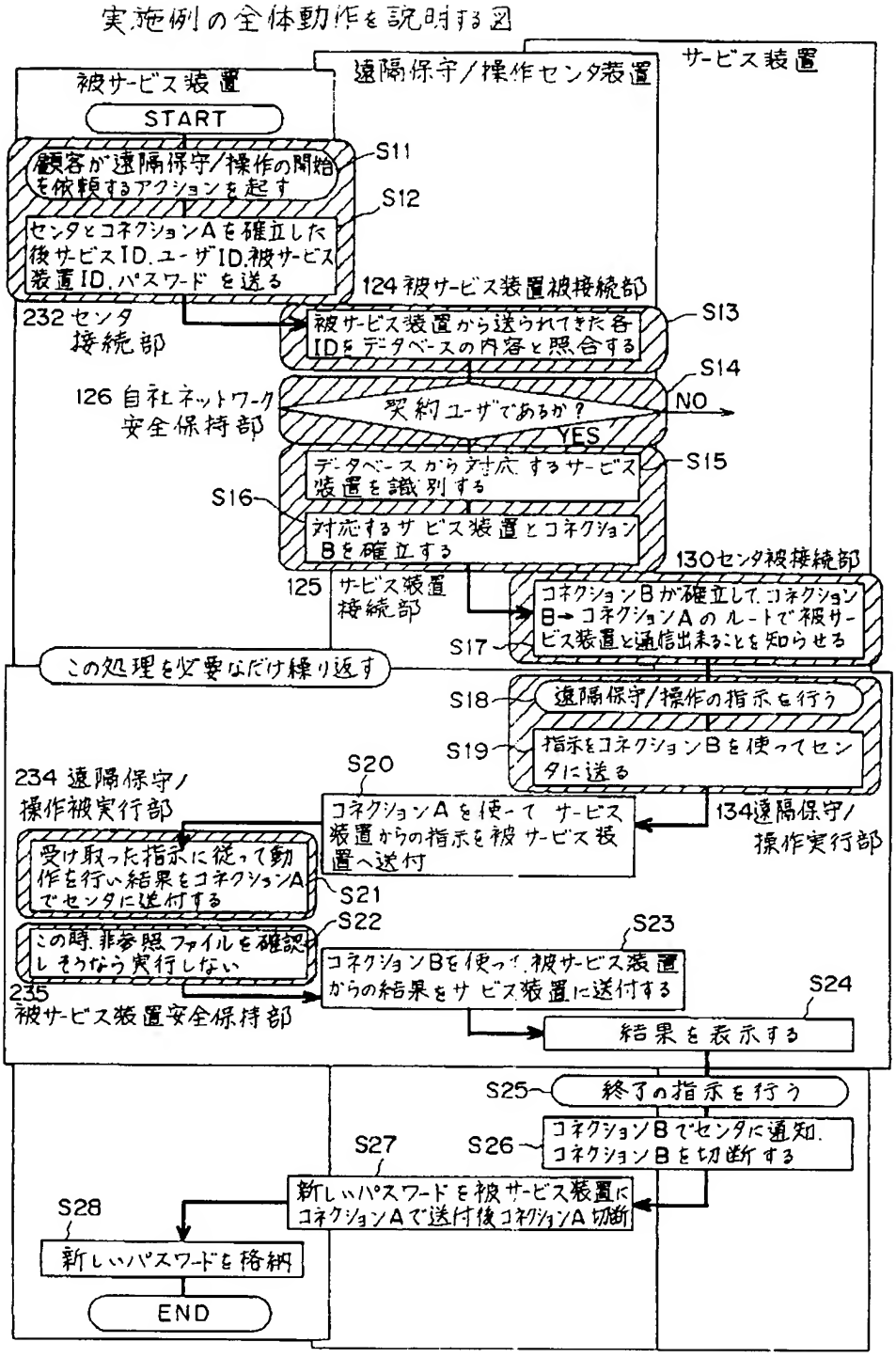


【図５】

本発明の一実施例である遠隔保守及び遠隔操作を行うシステムの全体構成を示す図

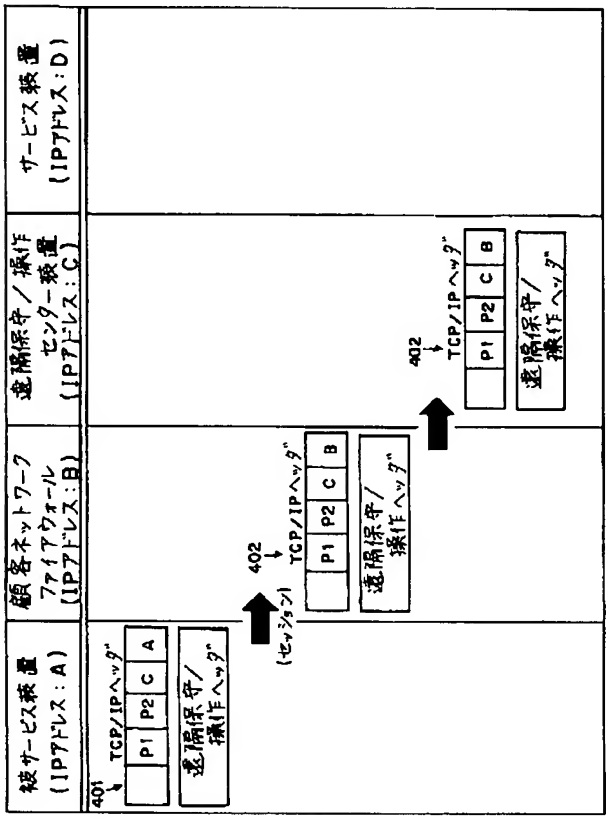


【図6】


実施例の全体動作を説明する図
被サービス装置
遠隔保守/操作センタ装置
サービス装置
START
顧客が遠隔保守/操作の開始を依頼するアクションを起す
S11
センタとコネクションAを確立した後サービスID,ユーザID,被サービス装置ID,パスワードを送る
S12
124 被サービス装置被接続部
232 センタ接続部
被サービス装置から送られてきた各IDをデータベースの内容と照合する
S13
126 自社ネットワーク安全保持部
契約ユーザであるか?
S14
NO
YES
データベースから対応するサービス装置を識別する
S15
S16
対応するサービス装置とコネクションBを確立する
125 サービス装置接続部
130センタ被接続部
コネクションBが確立して,コネクションB→コネクションAのルートで被サービス装置と通信出来ることを知らせる
S17
この処理を必要なだけ繰り返す
S18
遠隔保守/操作の指示を行う
S19
指示をコネクションBを使ってセンタに送る
S20
234 遠隔保守/操作被実行部
コネクションAを使ってサービス装置からの指示を被サービス装置へ送付
134遠隔保守/操作実行部
受け取った指示に従って動作を行い結果をコネクションAでセンタに送付する
S21
S22
この時,非参照ファイルを確認しそうなら実行しない
S23
コネクションBを使って,被サービス装置からの結果をサービス装置に送付する
235 被サービス装置安全保持部
S24
結果を表示する
S25
終了の指示を行う
S26
コネクションBでセンタに通知,コネクションBを切断する
S27
新しいパスワードを被サービス装置にコネクションAで送付後コネクションA切断
S28
新しいパスワードを格納
END

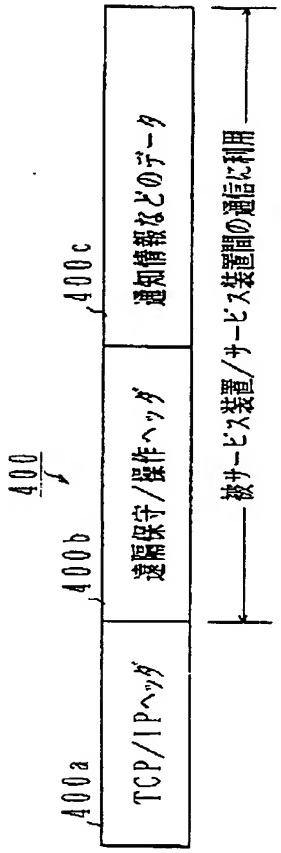
【図9】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その1）



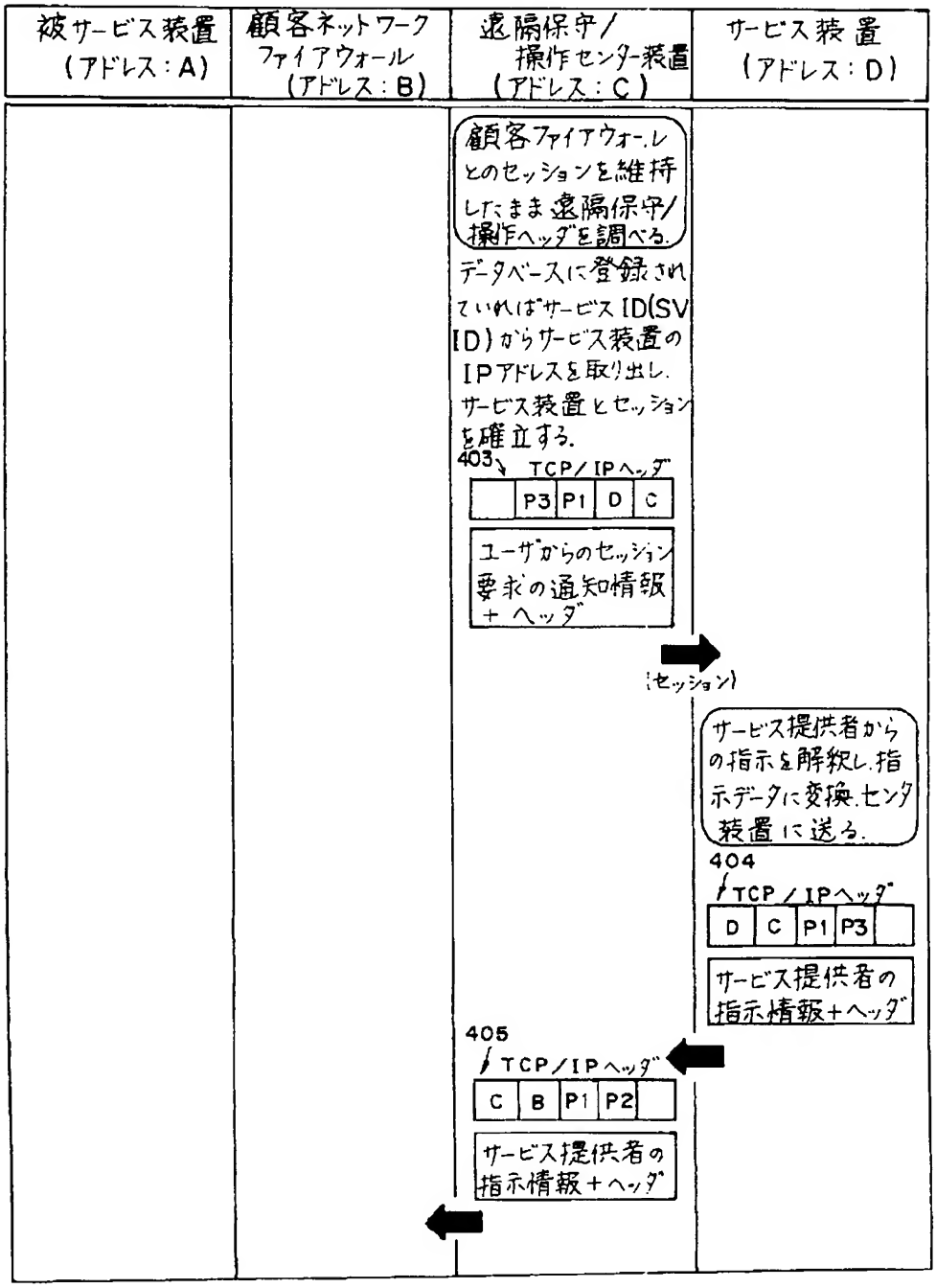

【図12】

図9～図11に示す動作中において、被サービス装置とサービス装置間で送受信されるパケットのフォーマットを示す図



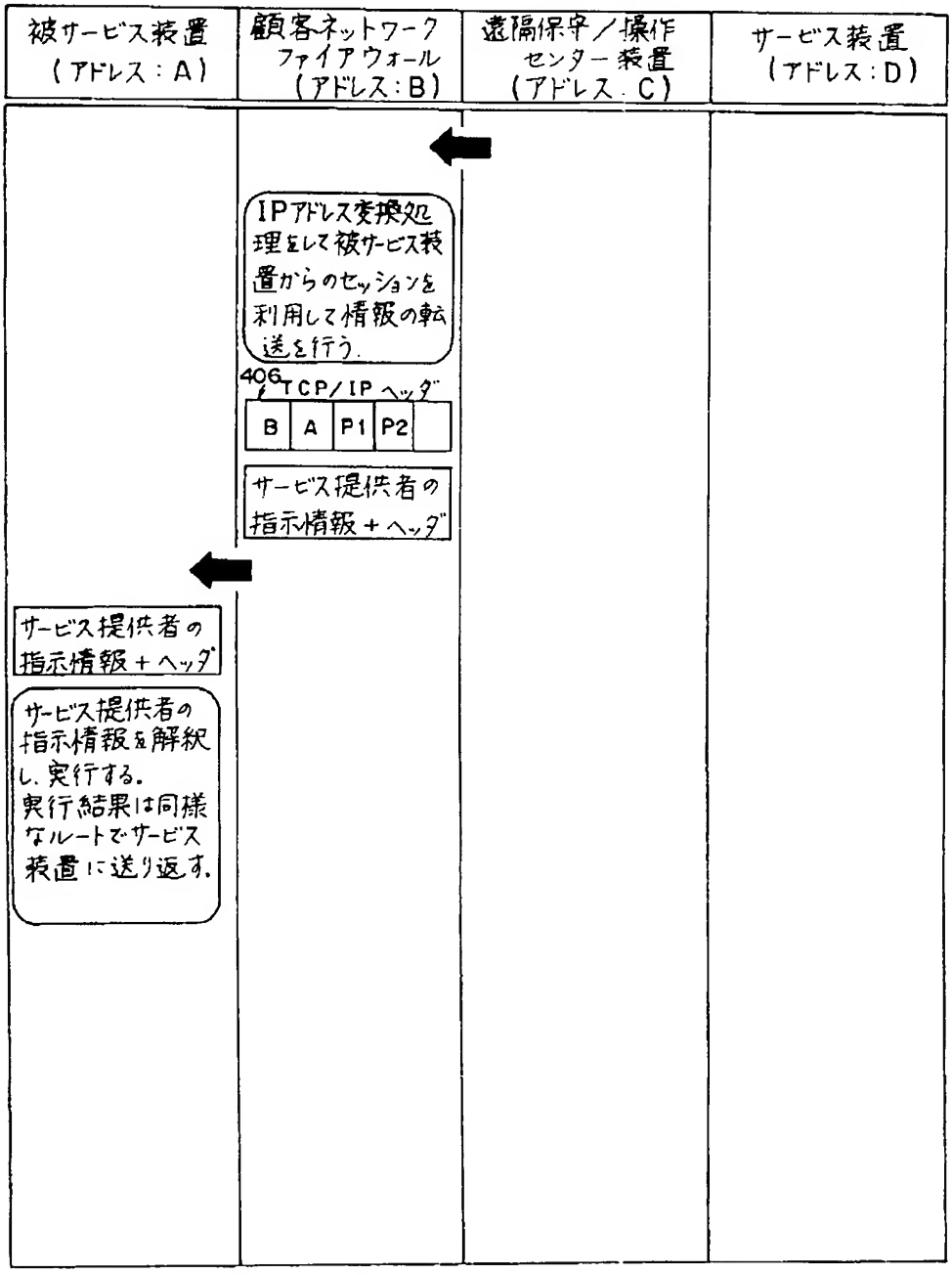
【図10】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その2）



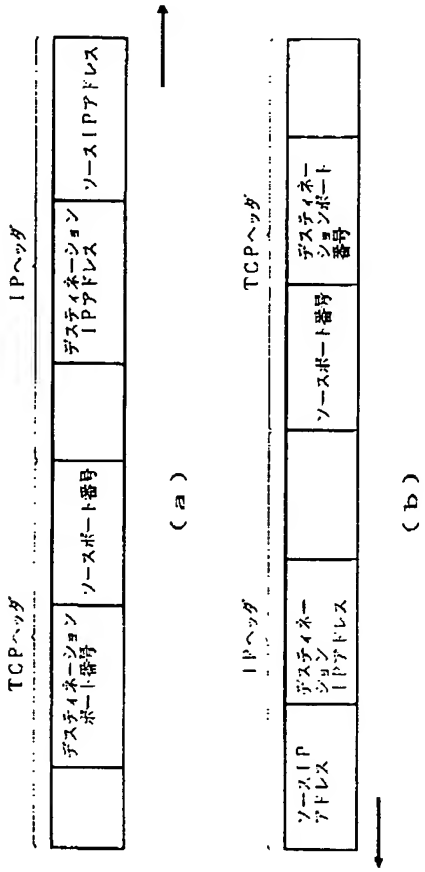
【図11】

図7に示すシステムでサービス装置が顧客の被サービス装置の遠隔保守／操作を実施する際に、両装置間で授受されるパケットの内容を示す図（その3）



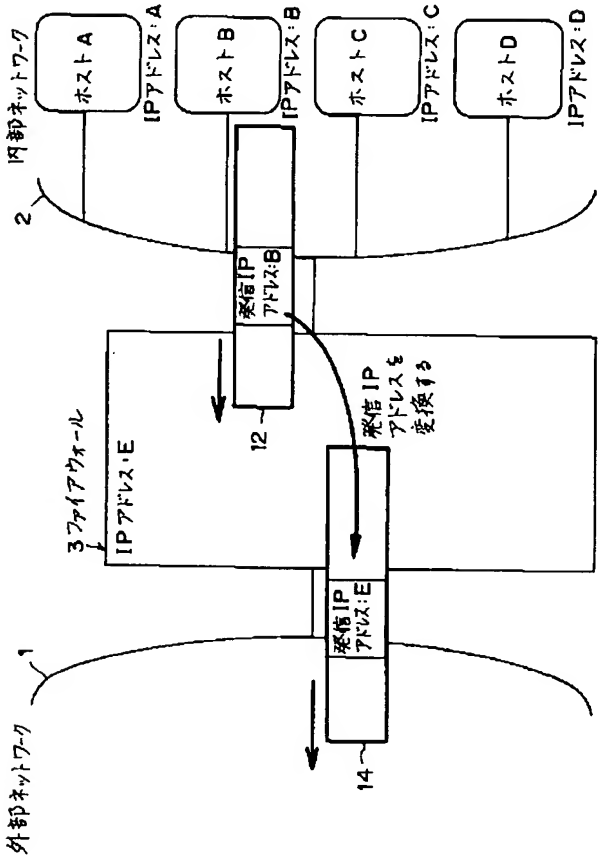
【図13】

図9および図11に示されたパケットのフォーマットを説明する図



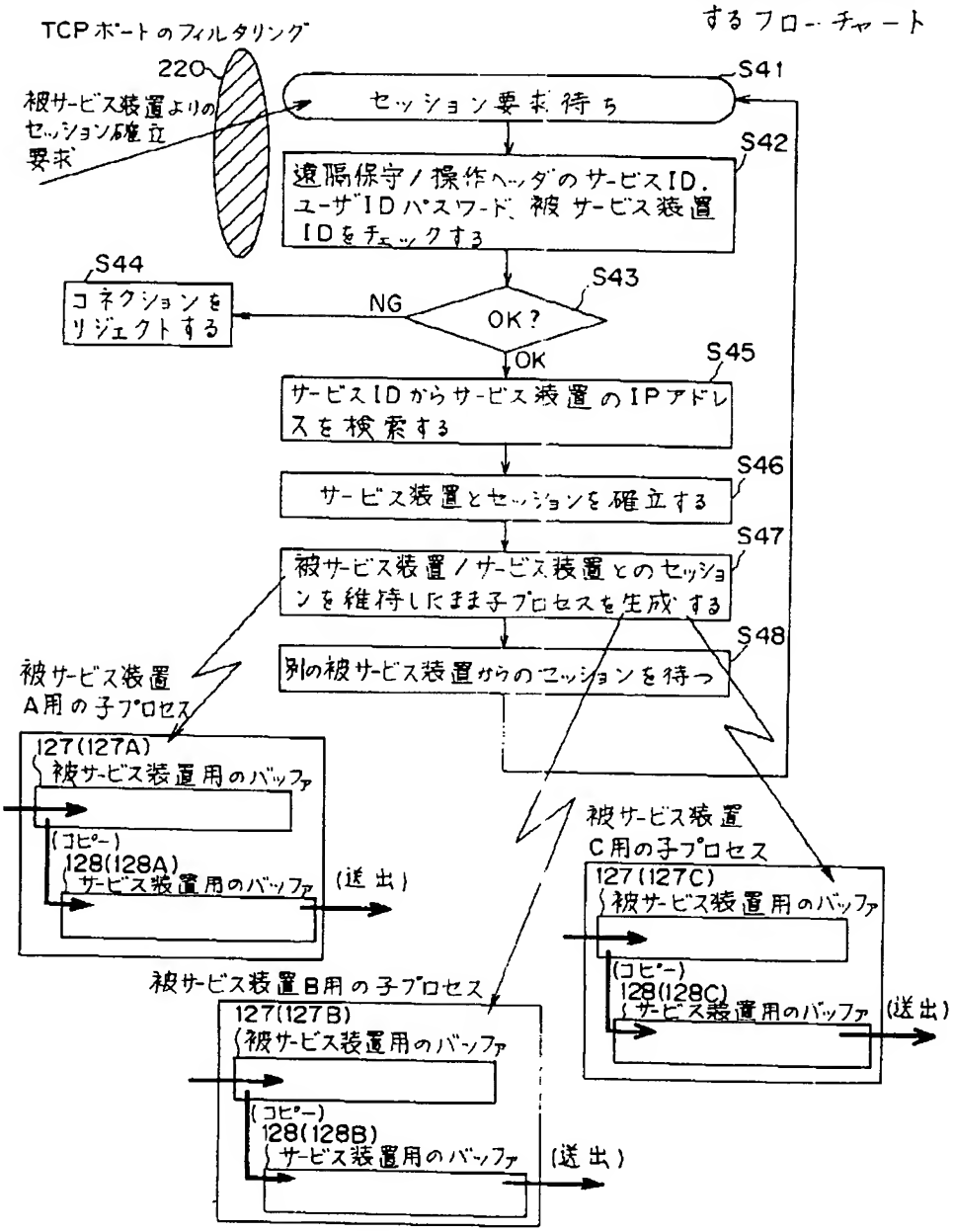

【図17】

ファイアウォールの第二の機能であるIPアドレス変換／中継機能を説明する図



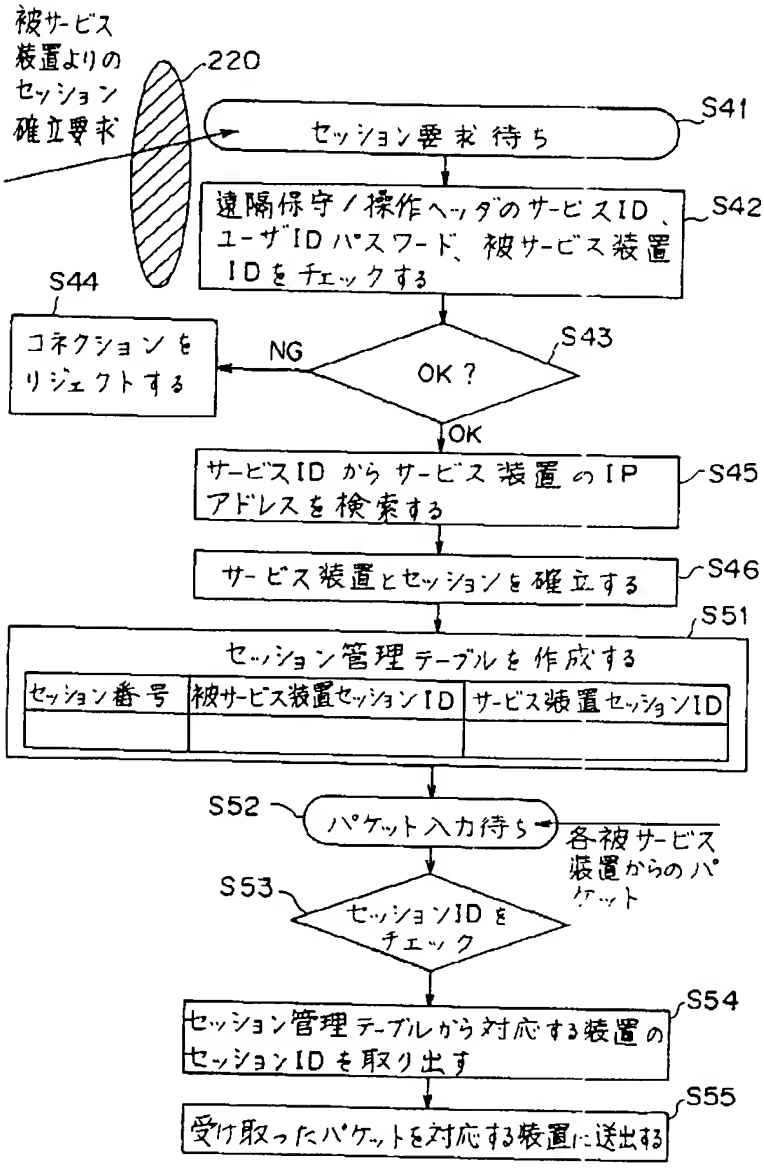
【図14】

遠隔保守／操作センタ装置が被サービス装置とサービス装置との間のパケット（IPデータグラム）の中継処理を実行する動作を説明するフローチャート



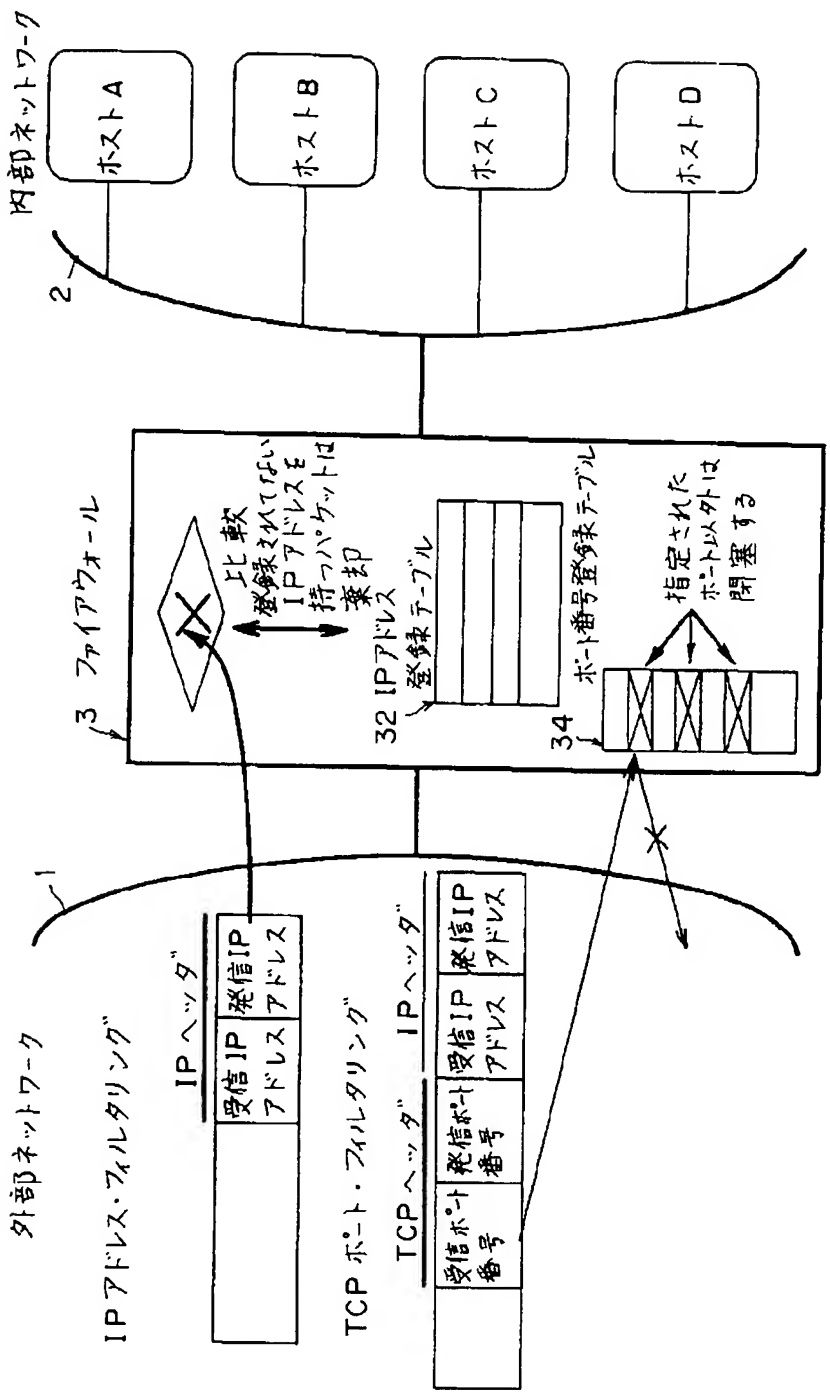
【図15】

図14のフローチャートに示された遠隔保守／操作センタ装置120のIP中継機能を別の観点から説明するフローチャート



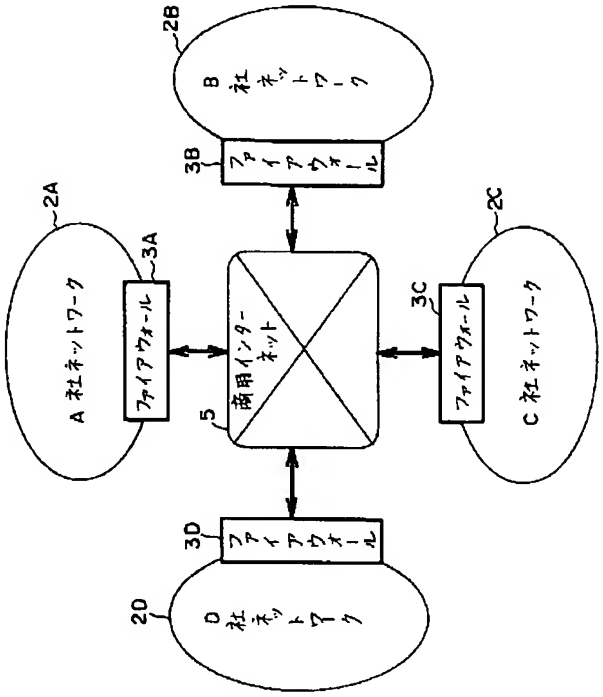
【図１６】

ファイアウォールのパケットフィルタリングゲートウェイ機能を説明する図



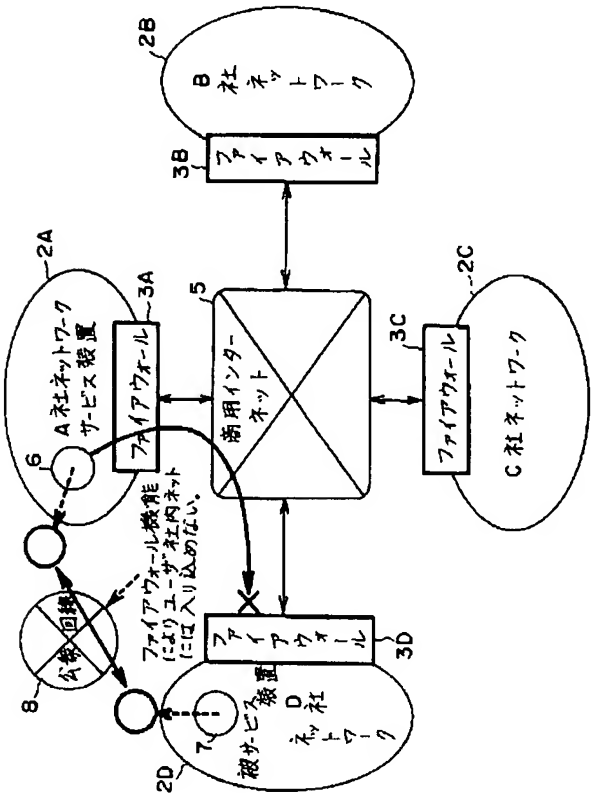
【図１８】

A社、B社、C社、及びD社の内部ネットワークがファイアウォールを介して、商用インターネットに接続されたシステムを示す図




【図１９】

図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施できない原因を説明する図



【図２０】

図18に示すシステムにおいて、A社の内部ネットワークに接続されたサービス装置がD社の内部ネットワークに接続された被サービス装置の遠隔保守／操作を実施する従来の方法を説明する図